



مركز البحوث والدراسات

دليل المسئول التنفيذي لحوكمة تقنية المعلومات

تحسين عمليات النظم من
خلال إدارة الخدمة وكويت
وآيتل

تأليف

روبرت ر. مولر

ترجمة

أ. محمد أحمد عبداللطيف - أ. عبدالله حسن كامل

راجع الترجمة

د. محمد بن عبدالله الشنيفي

بسم الله الرحمن الرحيم



مركز البحوث والدراسات

دليل المسئول التنفيذي لحوكمة تقنية المعلومات

تحسين عمليات النظم من
خلال إدارة الخدمة وكويت
وآيتل

تأليف

روبرت ر. مولر

ترجمة

أ. محمد أحمد عبداللطيف - أ. عبدالله حسن كامل

راجع الترجمة

د. محمد بن عبدالله الشنيفي

١٤٤٠ هـ - ٢٠١٩ م

بطاقة الفهرسة

③ معهد الإدارة العامة، ١٤٤٠هـ.

فهرسة مكتبة الملك فهد الوطنية أثناء النشر.
دليل المسئول التنفيذي لحكومة تقنية المعلومات تحسين
عمليات النظم من خلال إدارة الخدمة وكوبيت وآيتل.
أ - روبرت ر. مول؛ محمد عبداللطيف؛ عبدالله كامل -
الرياض، ١٤٤٠هـ

٦٧٢ ص؛ ١٧ سم × ٢٤ سم.

ردمك: ٩٩٦٠-١٤-٢٨٧-٦

١- تقنية المعلومات. ٢- تخزين واسترجاع المعلومات
٣- الحوكمة أ. عبداللطيف؛ محمد (مترجم) ب. كامل،
عبدالله (مترجم)
ج- العنوان.

ديوي ٠٢٥,٠٤ ١٤٤٠/٢٩٥١

رقم الإيداع: ١٤٤٠/٢٩٥١

ردمك: ٩٩٦٠-١٤-٢٨٧-٦

هذه ترجمة لكتاب:

Executive's Guide to IT Governance
Improving Systems Processes with Service Management
COBIT, and ITIL
ROBERT R. MOELLER

إهداء

إهداء لأفضل صديقة وزوجة، لويس مولر.

كانت لويس رفيقتي وشريكتي لأكثر من ٤٠ عاماً، سواء على مركبنا الشراعي في بحيرة ميشيغان، أو في التزلج في ولاية يوتا أو في أي مكانٍ آخر، أو أثناء زيارة المتاحف أو السفر إلى أماكن ممتعة حول العالم أو في بستانة الخضروات في الفناء الخلفي للمنزل أو مشاركتي إياها في طبخ أكالات من نتاج ما زرعناه.

قائمة المحتويات

الصفحة	العنوان
١٥	مقدمة
٢١	الجزء الأول: مفاهيم حوكمة تقنية المعلومات
٢٣	الفصل الأول: أهمية حوكمة تقنية المعلومات لجميع المؤسسات
٣١	الفصل الثاني: المفاهيم الأساسية للحوكمة وقواعد قانون ساربينز أوكسلي SOX ...
٣٢	قانون ساربينز أوكسلي SOX
٣٦	الباب الأول من قانون SOX: مجلس الإشراف المحاسبي على الشركات المساهمة PCAOB ..
٤٩	قواعد أخرى لقانون SOX - الباب الثاني: استقلالية المدقق
٥٦	الباب الثالث لقانون SOX: مسؤولية الشركة
٥٩	الباب الرابع لقانون SOX: تعزيز حالات الإفصاح عن البيانات المالية
٦٥	ما المقصود بحوكمة تقنية المعلومات
٨٠	ملاحظات
٨١	الفصل الثالث: حوكمة المؤسسات وأدوات الحوكمة وإدارة المخاطر والامتثال GRC ..
٨٢	الطريق نحو مبادئ فعالة للحوكمة وإدارة المخاطر والامتثال GRC
٨٥	أهمية الحوكمة في نموذج GRC
٨٨	عنصر إدارة المخاطر في نموذج GRC
٩١	نموذج GRC وامتثال المؤسسة
٩٦	أهمية ممارسات ومبادئ نموذج GRC الفعالة
٩٧	الجزء الثاني: أطر عمل لدعم حوكمة فعالة لتقنية المعلومات
	الفصل الرابع: حوكمة تقنية المعلومات ونظم الرقابة الداخلية طبقاً للجنة
٩٩	المنظمات الراعية (كوسو - COSO)
١٠١	أهمية أنظمة الرقابة الداخلية الفعالة ولجنة المنظمات الراعية (COSO)

١٢٦	إرشادات متابعة أنظمة الرقابة الداخلية (COSO)
١٢٨	تتمة: أهمية الرقابة الداخلية (COSO)
١٢٨	ملاحظات
١٢٩	الفصل الخامس: إطار كوبت (COBIT) ومعهد حوكمة تقنية المعلومات
١٣١	المقدمة التنفيذية للإطار كوبت
١٣٥	إطار العمل كوبت والعوامل المحركة له
١٣٨	المبدأ الأول لكوبت: إنشاء إطار متكامل لبنية تقنية معلومات
١٤١	المبدأ الثاني لكوبت: دوافع تحقيق قيمة لأصحاب المصلحة
١٤٤	المبدأ الثالث لكوبت: التركيز على سياق الأعمال
١٤٨	المبدأ الرابع لكوبت: عناصر تمكين إدارة المخاطر والحوكمة
١٥٢	المبدأ الخامس لكوبت: هياكل قياس أداء الحوكمة والإدارة
١٥٣	مطابقة عمليات كوبت مع أهداف تقنية المعلومات من خلال الجمع بينهما
١٥٨	استخدام كوبت في بيئة قانون ساربنز أوكسلي (SOX)
١٦٠	كوبت في دائرة الضوء
١٦١	ملاحظات
١٦٣	الفصل السادس: إرشادات إطار آيتل (ITIL) وإدارة خدمات تقنية المعلومات
١٦٤	أساسيات آيتل
١٦٩	عناصر إستراتيجية الخدمة في آيتل
١٧٧	تصميم الخدمة في آيتل
١٨٥	عمليات إدارة انتقال الخدمة في آيتل
١٩٠	عمليات تشغيل الخدمة في آيتل
١٩٧	حوكمة تقنية المعلومات وأفضل ممارسات تقديم الخدمة في آيتل
١٩٨	ملاحظة

١٩٩	الفصل السابع: معايير حوكمة تقنية المعلومات: أيزو ٩٠٠١ و ٢٧٠٠٢ و ٣٨٥٠٠
٢٠٠	معلومات أساسية عن معايير الأيزو
٢٠٤	معايير الأيزو ٩٠٠٠ لإدارة الجودة
٢٠٩	معايير الأيزو الخاصة بأمن تقنية المعلومات: أيزو ٢٧٠٠٢ و ٢٧٠٠١
٢١٦	معايير أيزو ٣٨٥٠٠ الخاص بحوكمة تقنية المعلومات
٢٢٤	ملاحظات
	الفصل الثامن: قضايا حوكمة تقنية المعلومات: إرشادات حول إدارة المخاطر وإدارة المخاطر المؤسسية الصادرة عن لجنة المنظمات الراعية (COSO ERM) والمجموعة المفتوحة للامتثال والأخلاقيات (OCEG)
٢٢٥	أساسيات إدارة المخاطر
٢٢٦	تعريفات إدارة المخاطر المؤسسية وأهدافها الصادرة عن لجنة المنظمات الراعية (COSO ERM): عرض محفوظة المخاطر
٢٤١	إطار إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية (COSO ERM) ..
٢٤٥	أبعاد أخرى في إطار (COSO ERM)
٢٧٢	"الكتاب الأحمر" لنموذج الحوكمة وإدارة المخاطر والامتثال التابع للمجموعة المفتوحة للامتثال والأخلاقيات (OCEG GRC)، وإدارة المخاطر، وحوكمة تقنية المعلومات
٢٧٣	ملاحظات
٢٨٠	الجزء الثالث: أدوات وتقنيات إدارة البنية التحتية لحوكمة تقنية المعلومات
٢٨١	الفصل التاسع: حوسبة سحابية وافتراضية وحوسبة محمولة متنقلة
٢٨٣	التعرف على الحوسبة السحابية
٢٨٦	نظم تقنية المعلومات وافتراضية إدارة التخزين
٢٩٦	قضايا حوكمة الهواتف الذكية وأجهزة تقنية المعلومات المحمولة
٣٠٩	ملاحظة
٣١٢	

٣١٣	الفصل العاشر: الحوكمة وإدارة أمن تقنية المعلومات وإدارة الاستمرارية
٣١٤	أهمية البيئة الفعالة لأمن تقنية المعلومات
٣١٦	مبادئ أمن تقنية المعلومات في المؤسسة: المعايير الأمنية المتفق عليها
٣٢٧	أهمية الإستراتيجية الأمنية الفعالة على مستوى المؤسسة
٣٣١	تخطيط استمرارية تقنية المعلومات
٣٣٤	خطط استمرارية الأعمال وحوكمة تقنية المعلومات
٣٤٣	ملاحظات
	الفصل الحادي عشر: معايير أمن البيانات الخاصة بصناعة بطاقات الدفع
٣٤٥	(PCI DSS) وقواعد أخرى لحوكمة تقنية المعلومات
	معلومات أساسية عن صناعة بطاقات الدفع وأمن البيانات PCI DSS والمعايير
٣٤٦	الخاصة بها
	قانون جرام ليتش بيلي (GRAMM-LEACH-BLILEY) في القواعد الخاصة
٣٦٠	بحوكمة تقنية المعلومات
	قانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة (HIPAA): العناية
٣٧٠	الصحية وأكثر
٣٨٦	ملاحظات
	الفصل الثاني عشر: بيان خدمات تقنية المعلومات: تحقيق قيمة أكبر من
٣٨٧	عمليات تشغيل تقنية المعلومات
٣٩١	أهمية بيان خدمات تقنية المعلومات
٣٩٦	دور بيان الخدمة في تنظيم أعمال مزود خدمات تقنية المعلومات
٣٩٩	محتوى بيان خدمات تقنية المعلومات وسماته
٤٠٢	إدارة بيان خدمات تقنية المعلومات

٤١١	الجزء الرابع: بناء أنظمة حوكمة تقنية معلومات فعالة ومراقبتها
	الفصل الثالث عشر: أهمية البنية الموجهة نحو خدمات تقنية المعلومات لنظم
٤١٣	حوكمة تقنية المعلومات
	تطبيقات البنية الموجهة نحو الخدمة (SOA) وتطبيقات تقنية المعلومات
٤١٤	المدفوعة بالخدمة
٤٢١	حوكمة البنية الموجهة نحو الخدمة وقضايا الرقابة الداخلية والمخاطر
٤٢٢	تخطيط وبناء مخطط تطبيق البنية الموجهة نحو الخدمة وتنفيذه
٤٣٥	البنية الموجهة نحو الخدمة وحوكمة تقنية المعلومات
٤٤٢	ملاحظات
٤٤٣	الفصل الرابع عشر: إدارة تهيئة ومحفظة تقنية المعلومات
٤٤٥	مفاهيم إدارة تهيئة تقنية المعلومات
٤٤٩	أفضل ممارسات إطار آيتل الخاصة بإدارة تهيئة تقنية المعلومات
٤٥٥	قاعدة بيانات إدارة التهيئة (CMDB): غالباً ما يكون مفهوماً صعباً
٤٥٨	إنشاء قاعدة بيانات إدارة التهيئة CMDB في المؤسسة
٤٦٥	إدارة محفظة تقنية المعلومات
	الفصل الخامس عشر: عمليات تنفيذ النظم التطبيقية وحوكمة تقنية
٤٧١	المعلومات
٤٧٣	دورة حياة تطوير النظم: إحدى التقنيات الأساسية لتطوير التطبيقات
٤٧٦	عمليات التطوير السريع في تقنية المعلومات: النمذجة (Prototyping)
٤٨١	تخطيط موارد المؤسسة وعمليات حوكمة تقنية المعلومات

٤٩١	الفصل السادس عشر: قضايا حوكمة تقنية المعلومات: إدارة المشاريع والبرامج
٤٩٢	عملية إدارة المشاريع
٤٩٥	معايير الدليل المعرفي لإدارة المشاريع PMBOK
٤٩٩	أسلوب آخر لإدارة المشاريع: برنس 2 2 Prince
٥٠٠	محفظة نظم تقنية المعلومات وإدارة البرامج
٥٠٧	مكتب إدارة البرامج (PMO)، أحد الموارد القوية للحوكمة
٥١٠	إدارة المشاريع ومكتب إدارة البرامج (PMO) وحوكمة تقنية المعلومات
٥١٠	ملاحظة
	الفصل السابع عشر: اتفاقيات مستوى الخدمات (SLAs) ومنتدى إدارة
	خدمات تقنية المعلومات (itSMF) وقيمة تقنية المعلومات (Val IT)
٥١١	وتعظيم استثمارات تقنية المعلومات
	أفضل ممارسات إدارة الخدمات طبقاً لإطار آيتل ومنتدى إدارة خدمات تقنية
٥١٣	المعلومات (itSMF)
٥٢٠	معايير المجموعة المفتوحة للامتثال والأخلاقيات OCEG
٥٣٢	قيمة تقنية المعلومات Val IT: تحسين قيمة استثمارات تقنية المعلومات ...
٥٤٥	ملاحظات
٥٤٧	الجزء الخامس: متابعة وقياس حوكمة إدارة المؤسسة ومجلس الإدارة
٥٤٩	الفصل الثامن عشر: إدارة محتوى المؤسسة
٥٥٠	خصائص إدارة المحتوى المؤسسي ومكوناتها الرئيسية في المؤسسة اليوم
٥٥١	عمليات إدارة المحتوى المؤسسي وحوكمة تقنية المعلومات
٥٥٧	خلق بيئة فعالة لنظام إدارة المحتوى المؤسسي في المؤسسة
٥٦٥	الفصل التاسع عشر: دور التدقيق الداخلي في الحوكمة
٥٦٦	تاريخ التدقيق الداخلي ومعلومات أساسية عنه

٥٧١	التدقيق الداخلي ومدقق تقنية المعلومات
٥٧٣	أنشطة التدقيق الداخلي ومسئوليته المرتبطة بحوكمة تقنية المعلومات
٥٨٢	معايير التدقيق الداخلي الخاصة بحوكمة تقنية المعلومات
٥٨٣	إجراءات التدقيق الداخلي الخاصة بحوكمة تقنية المعلومات
٥٩٠	ملاحظة
٥٩١	الجزء السادس: حوكمة تقنية المعلومات وأهداف المؤسسة
٥٩٣	الفصل العشرون: بناء ثقافة أخلاقية في محل العمل والحفاظ عليها
٥٩٣	أهمية بيانات المهمة (الرسالة)
٥٩٨	مدونة قواعد السلوك للمؤسسة
٦٠٩	المبلغون عن المخالفات وإدارات الخط الساخن
٦١٩	إطلاق برنامج أخلاقيات العمل وتحسين ممارسات الحوكمة المؤسسية
٦٢١	ملاحظة
٦٢٣	الفصل الحادي والعشرون: تأثير حوسبة وسائل التواصل الاجتماعي
٦٢٤	ما المقصود بحوسبة وسائل التواصل الاجتماعي؟
٦٢٨	أمثلة على وسائل التواصل الاجتماعي
٦٤١	نقاط ضعف حوسبة وسائل التواصل الاجتماعي في المؤسسة ومخاطرها
٦٥٠	ملاحظات
٦٥١	الفصل الثاني والعشرون: حوكمة تقنية المعلومات ودور لجنة تدقيق تقنية المعلومات
٦٥١	لجنة التدقيق التابعة للمؤسسة وحوكمة تقنية المعلومات
٦٥٦	مسؤوليات لجنة التدقيق تجاه حوكمة تقنية المعلومات
٦٥٨	اجتماعات لجنة التدقيق وقضايا حوكمة تقنية المعلومات
٦٦١	نبذة عن المؤلف
٦٦٣	المترجم في سطور

مقدمة

في ظل الظروف الاقتصادية الدائمة التغير التي يشهدها عالم اليوم والأنشطة التنظيمية المتزايدة، تصبح الحوكمة ذات أهمية متزايدة لجميع الشركات على اختلاف أحجامها، سواء كانت مؤسسات قطاع عام غير ربحية أو كيانات خاصة. وتتكون مفاهيم حوكمة المؤسسات من سلسلة من مجالات واسعة تغطي أنشطة المؤسسة التي تبدأ بالمساءلة الإدارية وإدارة المسؤوليات الائتمانية تجاه عملائها وموظفيها ومنظميها وغيرهم من أصحاب المصالح جميعهم. ويتطلب ذلك تطبيق عدد من الإرشادات والبرامج لضمان نزاهة الإجراءات الإدارية وحماية المؤسسة من الممارسات المخالفة والاحتيالية. كما تشتمل حوكمة المؤسسة أيضاً على عمليات الإدارة وسياساتها التي تعزز الكفاءة الإستراتيجية والاقتصادية للمؤسسة. وتتضمن إدارة الكفاءة الاقتصادية للمؤسسة الكيفية التي من خلالها ينوي نظام الحوكمة لديها تحسين النتائج وتحقيق الأهداف المرجوة، كما يدعو تعزيز الكفاءة الإستراتيجية للمؤسسة إلى تعزيز أهداف سياسة عامة للمؤسسة وإرسائها، تلك الأهداف التي لا تقاس دائماً من المنظور الاقتصادي مباشرة لكنها تشتمل على أمور مثل وضع برنامج أخلاقيات مؤسسية قوي وتحسين الجودة ورفاهية الموظفين.

ومن الطبيعي أن تحتاج الحوكمة المؤسسية الفعالة إلى مهارات إدارية قوية لاتخاذ قرارات مهمة وتشكيل القيادة. كما تحتاج وبشكل كبير إلى نظم وعمليات تقنية المعلومات على وجه الخصوص. ويمثل هذا المجال المهم، حوكمة تقنية المعلومات، الموضوع الشامل لهذا الدليل التنفيذي.

وفي الأيام الأولى لعمليات تقنية المعلومات ونظمها، كانت الإدارة العليا للعمليات التشغيلية غالباً ما توكل عمليات كثيرة من عمليات تقنية المعلومات للمتخصصين المسؤولين عن بناء موارد تقنية المعلومات في المؤسسة وتشغيلها وصيانتها. وبينما كثر الحديث وقتها عن ضرورة إشراك الإدارة ومستخدمي نظم تقنية المعلومات مع متخصصي ومطوري موارد تقنية المعلومات، فإن إدارة العمليات كانت تتعرض دائماً لخيبات أمل. فالمبادرات الجديدة لتقنية المعلومات وقتها لم تحقق في الغالب أهدافها المرجوة المعتمدة أو حققتها في وقت متأخر أو احتوت على نقاط ضعف في أمن المعلومات والرقابة الداخلية، أو أنها لم تعد مطلوبة إما بسبب سوء التخطيط أو تقديرات احتياجات الإدارة. ولتحسين تلك الأمور اليوم، تظهر الحاجة إلى عمليات أفضل لإدارة وتنسيق جميع جوانب موارد تقنية المعلومات في المؤسسة، أي الحاجة إلى حوكمة تقنية المعلومات.

هذا الكتاب هو دليل للسلطة التنفيذية يتناول هذا المفهوم المهم لحوكمة تقنية المعلومات. ولا نركز هنا على قيام متخصصي تقنية المعلومات بتركيب معدات هاردوير وبرمجيات وتوصيلات شبكات خاصة بتقنية المعلومات، ولا على الموارد المهمة مثل المدققين الداخليين الذين يختبرون عمليات تقنية المعلومات ويراجعونها. لكننا نركز على السلطة التنفيذية في المؤسسة التي يكون لديها بعض الفهم لعمليات تقنية المعلومات، لكنها تكون مهتمة أكثر بمعرفة المزيد عن القضايا والعمليات الضرورية المهمة في إدارة موارد وأنظمة تقنية المعلومات بكفاءة وكذلك الاستفادة منها في بيئة اليوم المتصلة بالإنترنت.

ويهدف هذا الكتاب إلى تقديم معلومات أساسية عالية المستوى عن نوع من القضايا المتعلقة بحوكمة تقنية المعلومات التي تعتبر مهمة لمؤسسات الأعمال وللمدير التنفيذي اليوم. ونأمل أن نزود الجهة التنفيذية في المؤسسة بمعلومات عامة وكافية تتمكن من خلالها من تكوين فهم أكبر عن قضايا حوكمة تقنية المعلومات المهمة هذه الأيام ولتكون قادرة أيضاً على طرح أسئلة أفضل لتحقيق فهم أكبر لهذه القضايا ولاتخاذ قرارات فعالة فيما يتعلق بمسائل حوكمة تقنية المعلومات تلك. فعلى سبيل المثال: نشر اليوم في كثير من الأحيان في أدبيات الأعمال التجارية إلى مصطلح الحوسبة السحابية (Cloud Computing). وسيقدم لنا الفصل التاسع نظرة عامة عن الحوسبة السحابية وسبب أهميتها في حوكمة تقنية المعلومات الفعالة. وبالمثل، سنقدم مفهوم اتفاقيات مستوى الخدمة (SLAs)، وهي عادة عقود غير رسمية تُبرم بين مستخدمي أو أصحاب موارد تقنية المعلومات وإدارة تقنية المعلومات. وهدفنا هنا هو مساعدة السلطة التنفيذية في المؤسسة ليكون لديها فهم أكبر عن سبب أهمية اتفاقيات مستوى الخدمة وكيفية تبنيها في المؤسسات وإدارتها على اختلاف أحجامها وأنواعها، وكيف يمكن استخدامها لتحسين عمليات حوكمة تقنية المعلومات.

وقد قُسمت فصول هذا الكتاب لستة مواضيع أو أجزاء رئيسية. كل جزء من هذه الأجزاء والفصول التي يحتويها يعتبر وحدة متكاملة في العموم، ويلخص قضايا حوكمة تقنية المعلومات التي تخص هذا الجزء، ونأمل أن تتمكن من خدمة الجهة التنفيذية بالمؤسسة من خلال تزويدها بمعلومات كافية عالية المستوى لفهم كل من قضايا حوكمة تقنية المعلومات تلك ومفاهيمها.

الجزء الأول: مفاهيم حوكمة تقنية المعلومات:

تزودنا فصول هذا الجزء بمقدمة شاملة عن مفهوم حوكمة تقنية المعلومات وكيفية تطبيقها على مؤسسات الأعمال عموماً، وعلى موارد تقنية المعلومات لهذه المؤسسات لاحقاً. ويحتوي هذا الجزء على فصل يصف أهمية قواعد قانون ساربينز أوكسلي (Sarbanes-Oxley Act (SOX) rules وتأثيرها بوصفها مجموعة من التشريعات تحوي القواعد العامة لضبط المؤسسات المالية وغيرها من نظم الرقابة الداخلية التي وضعت للمرة الأولى في الولايات المتحدة بدايات هذا القرن، أما الآن فهي مستخدمة تقريباً في جميع أنحاء العالم. ويختتم هذا الجزء بفصل يشرح قضايا شاملة لنظام الحوكمة والمخاطر والامتثال وهي ما تعرف بقضايا جي آر سي (GRC)، وهو مفهوم مهم ومصطلح شائع في العديد من النقاشات الإدارية في مؤسسات اليوم.

الجزء الثاني: أطر عمل لدعم حوكمة فعالة لتقنية المعلومات:

بالإضافة إلى المعايير والمفاهيم القيمة لحوكمة تقنية المعلومات، تحتاج الجهة التنفيذية في المؤسسة لفهم بعض أطر العمل المهمة لحوكمة تقنية المعلومات وحوكمة المؤسسة بأكملها. كما يحتوي هذا الجزء على فصل يقدم لمحة أو نظرة عامة عن إطار الرقابة الداخلية للجنة المنظمات الراعية (COSO) ويوضح سبب أهمية هذا الإطار بالنسبة لحوكمة فعالة لتقنية المعلومات. ويحتوي هذا الجزء أيضاً على فصل يقدم لمحة أو نظرة عامة ومقدمة عن أهداف ضوابط المعلومات والتقنيات ذات الصلة وهو ما يعرف بمصطلح كوبت (COBIT)، كما يدعم هذا الفصل توجيهات صادرة من معهد حوكمة تقنية المعلومات. ويمثل كل من ذلك مفاهيم مهمة في الرقابة الداخلية، ويجب أن يكون المسئول التنفيذي في المؤسسة مدركاً لتلك المفاهيم ولسبب أهميتها في حوكمة تقنية المعلومات.

ويحتوي هذا الجزء أيضاً على فصل يقدم مفهوماً مهماً آخر في حوكمة تقنية المعلومات، يعرف بمكتبة البنية التحتية لتقنية المعلومات آيتل (ITIL)، وهو عبارة عن المواد الإرشادية لأفضل ممارسات إدارة جميع جوانب موارد تقنية المعلومات في المؤسسة. وسيتناول هذا الفصل أيضاً منتدى إدارة خدمة تقنية المعلومات بوصفه مرتبطاً بمكتبة البنية التحتية لتقنية المعلومات، هذا المنتدى الذي يعد منظمة احترافية هامة تقدم دليلاً إرشادياً لحوكمة تقنية

المعلومات. ويجب على المسئول التنفيذي بالمؤسسة الذي يضطلع بمسؤوليات إدارة عمليات تقنية المعلومات أن يتمتع بمستوى فهم جيد لتلك المواد الإرشادية واستخداماتها في إحدى إدارات تقنية المعلومات وكيفية دعمها لحوكمة تقنية المعلومات لتكون أكثر كفاءة.

كما تقدم فصول الجزء الأول من هذا الكتاب إطارين مهمين في حوكمة تقنية المعلومات. أولاً: سنباش عدة معايير أيزو (ISO)، المنظمة العالمية للمعايير، ومجموعة من المواد الإرشادية المهمة لحوكمة تقنية المعلومات. وسنقدم أيضاً ما يعرف بـ (OCEG) أو المجموعة المفتوحة للامثال والأخلاقيات ومجموعة من إرشادات إدارة المخاطر. ولابد هنا من فهم كل من معايير الأيزو لحوكمة تقنية المعلومات والمجموعة المفتوحة للامثال والأخلاقيات (OCEG) لتنفيذ ممارسات حوكمة فعالة لتقنية المعلومات. ومن المفترض أن تساعد هذه الأطر مدير الشركة على فهم بعض قضايا حوكمة تقنية المعلومات الهامة.

الجزء الثالث: أدوات وتقنيات إدارة البنية التحتية لحوكمة تقنية المعلومات:

تشمل البنية التحتية لتقنية المعلومات جميع الأشخاص والموارد اللازمة لتشغيل تقنية المعلومات في المؤسسة وإدارتها، متضمناً ذلك أجهزة الخوادم وأخصائي أمن تقنية المعلومات وجميع الأشخاص والمعدات اللازمة لإدارة شبكة الاتصالات. ويناقش فصل في هذا الجزء العديد من التقنيات الأحدث والمهمة التي تتحكم في تغير عالم تقنية المعلومات اليوم، مثل مفاهيم الحوسبة السحابية ومفهوم الافتراضية. وسنتحدث عن هذه المفاهيم وقضايا أخرى ذات صلة، كما سنباش سبب أهميتها لحوكمة تقنية المعلومات.

وتتعرض البنية التحتية لتقنية المعلومات لنوعية من التهديدات على مستوى الأمن والسلامة، مثل تعرضها لهجوم غير متوقع من إحدى البرامج التخريبية أو عدم القدرة على استعادة الأعمال بسبب قصور في أنظمة النسخ الاحتياطي أو انتهاكات كلمات المرور مما يسبب اختراق البيانات السرية. ويوجد فصل هنا يتحدث عن قضايا مهمة لكفاءة حوكمة تقنية المعلومات، وهي قضايا تخطيط أمن تقنية المعلومات واستمراريتها. كما يوجد فصل آخر هنا يتناول بعض القواعد والأنظمة الأمنية لتقنية المعلومات الأكثر أهمية لتأسيس حوكمة تقنية معلومات ذات كفاءة عالية في المؤسسة.

ثم ننهي هذا الجزء بفصل يتناول أساليب تحقيق قيمة أكبر لعمليات تقنية المعلومات التي يجب أن تتضمن عمليات تُدار وتُراقب بشكل جيد وعمليات تقنية معلومات ذات كفاءة وجدوى اقتصادية. ويجب على الإدارة بجميع مستوياتها أن تتمتع بمستوى فهم عام لآلية تطبيق هذه القضايا والاستفادة منها. وسيطرح هذا الفصل أيضاً بعض التوجيهات من وجهة نظر إدارة تقنية المعلومات.

الجزء الرابع: بناء أنظمة حوكمة تقنية معلومات فعالة ومراقبتها:

بالإضافة إلى أدوات وعمليات البنية الأساسية لتقنية المعلومات التي ذكرت في الجزء السابق، فإن فصول هذا الجزء تناقش طرق بناء عمليات حوكمة تقنية معلومات فعالة في النظم والتطبيقات التي تتبناها المؤسسات. ويتناول أحد الفصول هنا بشكل خاص أهمية ما تعرف عموماً بأنها البنية الموجهة نحو الخدمة (SOA)، وهي الطريقة الأكثر شيوعاً واستخدماً اليوم لبناء تطبيقات جديدة وتنفيذها، تلك التطبيقات التي تمثل عمليات مختلفة تماماً عن العمليات التقليدية القديمة المتبعة مسبقاً في تطوير التطبيقات. وتتناول الفصول الأخرى في هذا الجزء قضايا حوكمة تقنية المعلومات اللازمة لإدارة الأنظمة وتغييرات العمليات وضوابط المراجعة بالإضافة إلى الحديث عن الطرق المستخدمة في تطبيق النظم المتكاملة التي تقدم حوكمة لعمليات تقنية المعلومات وإدارة لها بشكل أفضل.

ويوجد فصل في هذا الجزء يتحدث عن الأدوات والوسائل المستخدمة في إدارة المشاريع والبرامج. ويجب أن تدرك الإدارة بمختلف مستوياتها أهمية وقيمة كل من الإدارة الجيدة للمشاريع ووسائل الرقابة المستخدمة لتعزيز عمليات حوكمة تقنية المعلومات. ويأتي الفصل الأخير في هذا الجزء ليتحدث عن اتفاقيات مستوى الخدمة، حيث يتناول معايير ومقاييس الأداء الرسمية بين موارد تقنية المعلومات ومستخدميها، وهي إحدى الأدوات المهمة للغاية لحوكمة تقنية المعلومات.

الجزء الخامس: متابعة وقياس حوكمة إدارة المؤسسة ومجلس الإدارة:

ركزت معظم الفصول السابقة على تمكين المسئول التنفيذي لتقنية المعلومات من فهم وتنفيذ عمليات حوكمة تقنية المعلومات الفعالة في عمليات تقنية المعلومات بالمؤسسة

وأنظمتها. أما فصول هذا الجزء فتركز على دور التدقيق الداخلي في المؤسسة، حيث يحتوي هذا الجزء على فصل يوضح أهمية التدقيق الداخلي لحوكمة تقنية المعلومات. كما يحتوي هذا الجزء أيضاً على فصل يتناول طرق إدارة الوثائق من منظور المسئول التنفيذي لتقنية المعلومات متضمناً أهمية قضايا حفظ محتوى البيانات وإدارتها.

الجزء السادس: حوكمة تقنية المعلومات وأهداف المؤسسة:

يركز هذا الجزء الأخير من كتابنا على بعض الإرشادات لوضع ثقافة أخلاقية في بيئة العمل ومواصلة العمل بمقتضاها، الأمر الذي يمكن اعتباره من العناصر الهامة في حوكمة تقنية المعلومات. كما يحتوي هذا الجزء على فصل يتحدث عن أهمية تطبيقات حوسبة شبكة التواصل الاجتماعي - كثيرة الاستخدام هذه الأيام كفيسبوك مثلاً - ومدى تأثيرها في حوكمة تقنية المعلومات. أما الفصل الأخير من هذا الكتاب فيحتوي على توجيهات حول كيفية استخدام حوكمة تقنية المعلومات لتحقيق القيمة المرجوة من استخدام تقنية المعلومات.

ركزت هذه الفصول على حاجات الإدارة التنفيذية العليا للمؤسسة واهتماماتها. وسنبداً كل فصل من الفصول التالية بالحديث عن أهمية عنوان الفصل من منظور حوكمة تقنية المعلومات. ثم سنتحدث عن أدوات ووسائل تنفيذ عمليات حوكمة معينة وطرق قياس مدى نجاحها. وبالإضافة إلى هذه الفصول المخصصة للحديث عن الموضوعات المحددة التي أشرنا إليها، فإن هناك فصولاً أخرى ستتناول بالشرح عناصر مهمة من عمليات إدارة خدمة تقنية المعلومات وكوبت (COBIT) وآيتل (ITIL). كما سنحاول الربط بين جميع القضايا الخاصة بحوكمة تقنية المعلومات وبين الضوابط والمخاوف العامة لحوكمة المؤسسة.

إن الهدف العام من هذا الكتاب ليتمثل في مساعدة كبار مديري المؤسسات على فهم أهمية قضايا حوكمة تقنية المعلومات بشكل أفضل وعلى تطبيقها في مؤسساتهم، لتكون نتيجة ذلك الوصول إلى نظم وعمليات أقوى لكل من تقنية المعلومات والمؤسسة بكاملها.

الجزء الأول

مفاهيم حوكمة تقنية المعلومات

الفصل الأول

أهمية حوكمة تقنية المعلومات لجميع المؤسسات

كان الظهور الأول لتطبيقات تقنية المعلومات والحاسبات بشكل أساسي في عالم الأعمال مطلع ستينيات القرن العشرين في الولايات المتحدة وأوروبا. فقد كانت وقتها تقنية أعمال جديدة صاحبها قيام العديد من الشركات بتقديم عروض تنافسية لمنتجاتها من المعدات الحاسوبية والبرمجيات للشركات الرئيسية الكبرى ذلك الوقت. وقد سارعت الشركات على اختلاف مستوياتها لمواكبة تلك التقنية الحديثة، فضلاً عن الاستثمارات الضخمة التي خُصصت لتثبيت نظم جديدة وتوظيف مبرمجين ومحللين لبنائها وإطلاقها وتدريبهم على ذلك. وعلى الرغم من وقوع بعض الإخفاقات على طول الطريق، فإننا جميعاً، وفي هذه الأيام نستخدم تلك النوعيات من المنتجات البرمجية والمعدات الحاسوبية ونستفيد منها.

واليوم نجد أن نظم تقنية المعلومات المدعمة بتقنيات دائمة التغير والتطور تعد بمثابة العنصر الأساسي في الغالب لجميع أنشطة الأعمال. ومع ذلك، نجد أن أنشطة تقنية المعلومات التي نمارسها ليست مدعمة ببعض من المعايير والإجراءات نفسها الموجودة في مجالات أعمال أخرى. فعلى سبيل المثال، يتم دعم نظم المحاسبة والمعايير المالية من خلال مبادئ محاسبية متعارف عليها يقوم بمراجعتها مدققون مستقلون، فضلاً عن أنها تخضع لقواعد محاسبة مالية حكومية كقواعد هيئة الأوراق المالية والبورصة في الولايات المتحدة الأمريكية. كما توجد قواعد مشابهة لأفضل الممارسات والمعايير الخاصة بمجالات أنشطة أعمال أخرى كما هو الحال في كثير من مجالات التسويق ومراقبة الجودة. وليس هذا هو حال عمليات تقنية المعلومات ونظمها. وعلى الرغم من حقيقة أن عمليات تقنية المعلومات تواجه هذه الآونة متطلبات متزايدة فيما يخص الامتثال المهني والحكومي فضلاً عن تعرضها لكم هائل من مخاطر النظم المرتبطة بذلك، فإن الحاجة مستمرة لتبني ممارسات أفضل في حوكمة تقنية المعلومات هذه الأيام.

كان مفهوم حوكمة تقنية المعلومات مجهولاً إلى حد كبير لعدة سنوات قليلة مضت. فقد كنا نرى حوكمة المؤسسات من منظور الأدوار والأنشطة التي تقوم بها الإدارة العليا ومجلس الإدارة، في حين كنا لا نرى إدارات تقنية المعلومات في هذه المؤسسات القديمة إلا في شكل إدارات دعم فني مهمة للغاية وليست أنشطة رئيسية للأعمال. لقد تغير حقاً مفهومنا العام حول حوكمة المؤسسات في الولايات المتحدة في السنوات الأولى من القرن الحالي، وذلك بعد الإخفاق الذي تعرضت له إحدى كبرى الشركات الأمريكية والتي تدعى إنرون (Enron). الأمر الذي فاجأ الجميع ولم يكن متوقعاً على الإطلاق لدرجة قيام الهيئات التنظيمية الحكومية في الولايات المتحدة بإجراء تحقيق في هذا الأمر واكتشفت غياب العديد من الممارسات المالية وممارسات حوكمة الشركات. الأمر الذي أدى إلى فرض قانون ساربنز أوكسلي [Sarbanes-Oxley (SOX)] في الولايات المتحدة الأمريكية. وقد كان لهذه القواعد التشريعية الأثر الرئيسي على الممارسات المتعلقة بإعداد التقارير المالية وحوكمة الشركات، وذلك في الولايات المتحدة الأمريكية أولاً وبعدها في جميع أرجاء العالم. وقد كان لقانون ساربنز أوكسلي أيضاً دور رئيسي فيما يتعلق بالحاجة لحوكمة تقنية المعلومات بشكل فعال.

وفي هذه الآونة يفكر كبار المديرين ومديرو تقنية المعلومات والممارسون في حوكمة تقنية المعلومات بطرق عديدة غير أنها مختلفة، إذ يرى البعض حوكمة تقنية المعلومات على أنها قواعد "قيادة وسيطرة" على مبادرات تقنية المعلومات، وأن واضعي تلك القواعد هم مدققون داخليون ومديرون تنفيذيون غير تقنيين ومستشارون خارجيون؛ في حين يراها آخرون مجرد آلية تستخدمها المؤسسة لتطبيق نهج الأخ الأكبر بفرض قيود تنازلية Top-Down Constraints على جميع أنشطة تقنية المعلومات. أما من منظور ممارس تقنية المعلومات الذي يبني النظم ويديرها بهدف تحسين إنتاجية الأعمال، فإننا نجد أحياناً أن حوكمة تقنية المعلومات تبدو وكأنها شرٌّ لا ضرورة له يعيق النواحي الإبداعية والإنتاجية المرتبطة بتقنية المعلومات في المؤسسات. على كل حال، فإن حوكمة تقنية المعلومات لا تتحكم في إدارة الشركة وإداراتها التقنية من خلال فرض لوائح ومعايير وسياسات صارمة، لكن الحوكمة الجيدة لتقنية المعلومات في المقابل لا تعدو إلا أن تكون مجموعة من السياسات وأفضل الممارسات التي يلزم أن تعمل باعتبارها قوة إستراتيجية

تجعل من الممكن تحسين العمليات التشغيلية للأعمال، وبتلك الصورة لحوكمة تقنية المعلومات نجد جميع المؤسسات بكل مستوياتها تتبناها، بل نراها تتجاوز حدود عمليات تقنية المعلومات المؤسسية.

وتتميز الحوكمة الجيدة لتقنية المعلومات بالتوافق مع المؤسسة بشكل إستراتيجي لدعم تطوير بنية تقنية معلومات تقدم قيمة مؤسسية مناسبة يمكن تعظيمها. تساعد حوكمة تقنية المعلومات في قياس نمو الأعمال ونجاحها وكذلك قياس صحتها المالية. تقدم الفصول التالية من هذا الكتاب نظرة جديدة وشاملة لحوكمة تقنية المعلومات والتي تتناول معايير أداء الأعمال المؤسسية الجوهرية إلى جانب العوامل المهمة للالتزام بالامتثال وإدارة المخاطر. ونظراً لأن الفصول التالية ستناقش جوانب مهمة لكل من تلك العوامل، فإننا سنشير إلى الحوكمة والمخاطر والامتثال بهذا الاختصار (GRC) وهي مجموع الحرف الأول لكل كلمة. وهو المصطلح الشائع استخدامه هذه الأيام في المطبوعات المتعلقة بالأعمال.

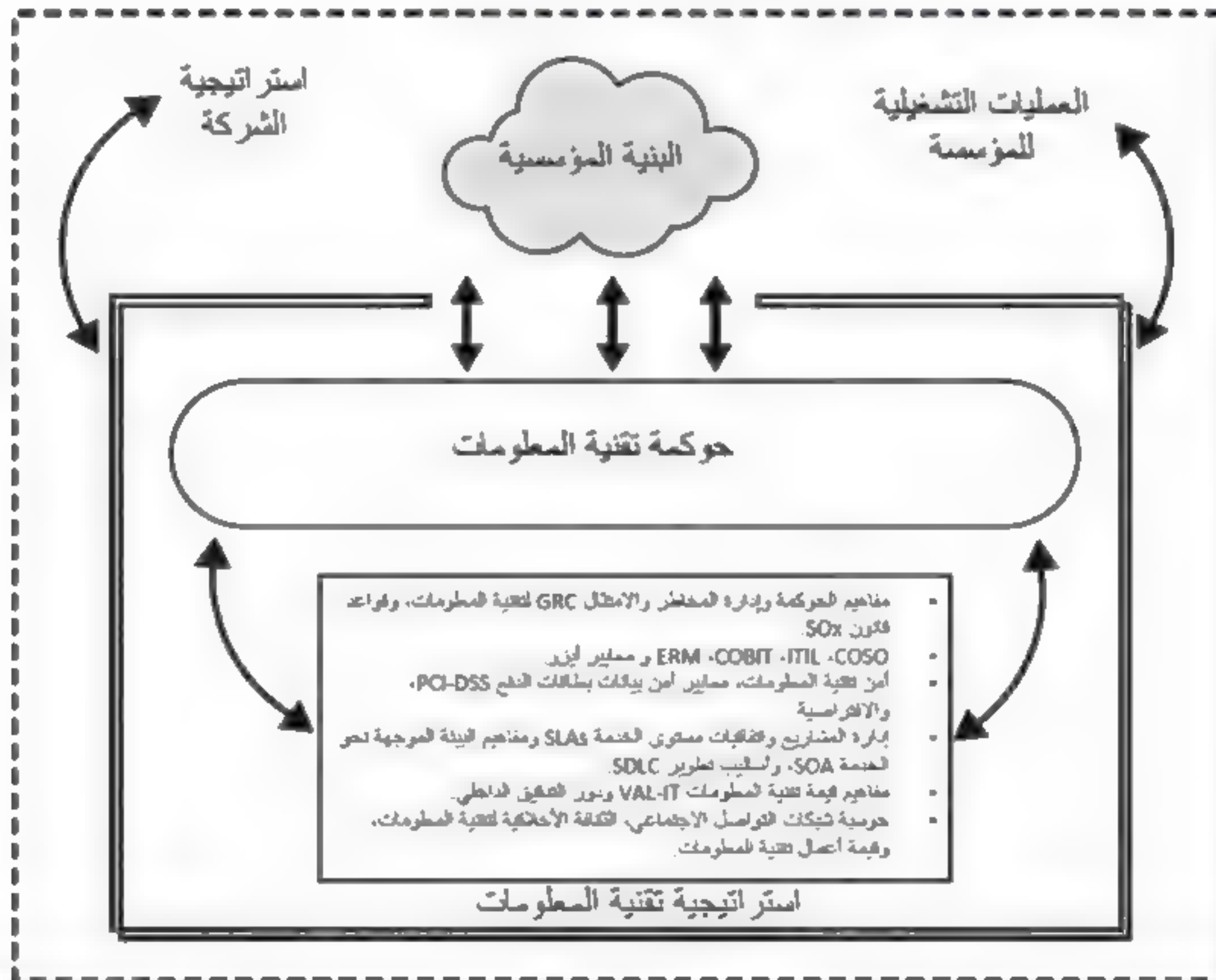
تبين حوكمة تقنية المعلومات الطريق الذي من خلاله تتمكن المؤسسة من تقديم قدرات أعمال لإنجاز مهام حرجية، وذلك باستخدام إستراتيجيات تقنية المعلومات وأهدافها وغاياتها. كما تهتم حوكمة تقنية المعلومات بتحقيق التوافق الإستراتيجي بين أهداف الأعمال وغاياتها من جهة واستغلال موارد تقنية المعلومات لديها من جهة أخرى لتحقيق النتائج المرجوة بكفاءة. يبين الشكل التوضيحي (١-١) هذا المفهوم لحوكمة تقنية المعلومات وكيفية توافقه مع جميع إستراتيجيات المؤسسة.

على الرغم من أن الشكل التوضيحي (١-١) عام جداً، إلا أنه يعرض مفاهيم حوكمة تقنية المعلومات - موضوع هذا الكتاب - في الوسط لتكون ضمن الإستراتيجيات والعمليات الشاملة للمؤسسة، وهو مفهوم أساسي دائماً يجب أخذه في الحسبان. وفي كثير من الأحيان قد يرى مدير تقنية معلومات متسلط أن أفكاره لتحسين نظم تقنية المعلومات وعملياتها وإدارتها تتجاوز في أهميتها غالباً الأنشطة الأخرى للمؤسسة، ولذا يجب علينا دائماً أن نعي أنه على الرغم من الأهمية القصوى لعمليات تشغيل تقنية المعلومات بالنسبة لجميع أعمال المؤسسة في كثير من الأحيان، فإنه يجب أن تنسجم تلك العمليات مع جميع أنشطة المؤسسة وإستراتيجياتها. وعلى الرغم من أن مدير إدارة تقنية المعلومات أو الرئيس

التنفيذي للمعلومات (Chief Information Officer (CIO ، قد يشعر بأن لديه المقترح الأصلح لعمل بعض التغييرات أو التحسينات في عمليات تقنية المعلومات؛ فإن هذا المقترح يجب أن يكون نافعاً لباقي أنشطة المؤسسة. فعلى سبيل المثال، قد يدرك الرئيس التنفيذي للمعلومات أهمية إبرام اتفاقيات مستوى الخدمة (Service Level Agreements (SLAs، أو عقود غير رسمية ما بين مستخدمي تقنية المعلومات ومقدميها، وهو ما سنتناوله في الفصل السابع عشر من هذا الكتاب، باعتبار ذلك وسيلة مناسبة لتحسين عمليات تقنية المعلومات وتطويرها. ولكن في حال عدم استحسان هذا المقترح من قبل الإدارة العليا، فإنه يجب على الرئيس التنفيذي للمعلومات أن يذعن لتوجه الإدارة العليا ولا يتوقف عن عمل تحسينات أخرى كلما أمكن ذلك.

شكل توضيحي (١-١)

مفاهيم حوكمة تقنية المعلومات



ولعل المقصد هنا يتركز في أن البنية المؤسسية لتقنية المعلومات هي التي تضع جميع قواعد الإطار العام لجميع أنشطة المؤسسة وحوكمة تقنية المعلومات. تقدم لنا الفصول التالية من هذا الكتاب عدة مجالات يمكن من خلالها تحسين نظم تقنية المعلومات وعملياتها. لكن مع استهداف تحسين حوكمة تقنية المعلومات في المؤسسة بالكامل يجب أن تنسجم تحسينات حوكمة تقنية المعلومات تلك مع الإطار العام لعمليات المؤسسة.

يشير الجزء الخاص بحوكمة تقنية المعلومات في الشكل التوضيحي (١-١) إلى سلسلة من الأنشطة الأخرى، يتوافق كل نشاط منها تقريباً مع موضوعات أحد الفصول الموجزة في مقدمة الكتاب والمفصلة في الفصول اللاحقة. وقد حاولنا في هذه الفصول أن نوجز العديد من القضايا المهمة لتحسين حوكمة تقنية المعلومات، تلك القضايا التي يجب أن ترتبط بشكل وثيق بجميع عمليات المؤسسة.

تعمل حوكمة تقنية المعلومات على توزيع السلطة على مختلف طبقات الهياكل التنظيمية داخل المؤسسة مع ضمان استخدام تلك السلطة بشكل سليم وحكيم. ولا نقصد هنا مجرد الهياكل الهرمية؛ بل يجب علينا دوماً أن نتذكر أن الهياكل الشبكية تسمح بالتخصصية وتشكيل الفرق وتشكيل بنية تحتية لدعم تلك الفرق. فالتخصصية تسمح لمجموع أجزاء المنظمة بأن يكون أكبر من الكل. كما يجب أن نتذكر أن حوكمة تقنية المعلومات ليست حكراً على المنظمات الكبرى، فالمؤسسات الأصغر تفتقر أيضاً إلى ممارسات جيدة لحوكمة تقنية المعلومات. ومع ذلك، يوجد بوضوح عدد أقل من نقاط الرقابة التي يلزم توظيفها في عمليات المؤسسات الصغرى في حين أن تركيزنا في فصول هذا الكتاب سينصب على المؤسسات الكبرى.

عندما نستعرض مفهوم حوكمة تقنية المعلومات كما أوردته الفصول التالية من هذا الكتاب، نجد أنها تؤثر في أداء الأعمال وتساعد وبشكل مثالي المؤسسة في أن تتفوق على منافسيها. ومن الموضوعات الأساسية هنا أن تعرف أن حوكمة تقنية المعلومات هي التي تحدد أداء الأعمال وخاصة أداء موارد تقنية المعلومات وقت تطبيقها لتحقيق الأهداف الإستراتيجية للأعمال. فالحوكمة الجيدة لتقنية المعلومات تؤدي مباشرة إلى إنتاجية أكبر وجودة أعلى ونتائج مالية أفضل، في حين أن الحوكمة السيئة لتقنية المعلومات تؤدي غالباً

إلى إهدار برمجي وبيروقراطية وانخفاض في الروح المعنوية وتدني الأداء المالي بشكل عام. ولإثبات أهمية الممارسات الجيدة لحوكمة تقنية المعلومات علينا أن ننظر إلى المؤسسات التجارية التقليدية التي تنتج السلع والخدمات لعملائها التقليديين، حيث نجد أن هؤلاء العملاء عموماً يرون الأعمال فقط عندما يتواصلون مع تلك المؤسسات لتقديم طلباتهم للحصول على تلك المنتجات أو على قيمة من خلال بيع تلك المنتجات أو إنتاجها أو لتقديم معلومات من خلال ملء الاستبيانات والتحليلات التسويقية. تعد كفاءة العمليات الداخلية للأعمال وتنسيقها هي ما تشكل خبرة العملاء بمجملها، وهذا في حد ذاته مجال من مجالات أداء الأعمال يجب قياسه وتطويره. وحتى تؤثر حوكمة تقنية المعلومات بشكل إيجابي في أداء الأعمال لابد أن تركز على مجمل عمليات الأعمال تلك وتستكشفها، تلك العمليات التي يتفاعل معها العملاء. وفي المقابل نرى أن الحوكمة السيئة لتقنية المعلومات تُخرج العميل من نظرها التزاماً منها بتطبيق بعض اللوائح والقوانين والمعايير والسياسات المفضلة والمعزولة. كما نلاحظ في سياق عمليات الأعمال الشمولية (من النهاية إلى النهاية) أن المكاسب المحلية الناتجة من كفاءة العمليات وإنتاجيتها لا تحقق في الغالب النتائج المرجوة. هذا بالإضافة إلى أن تطبيق اللوائح الخارجية على عمليات الأعمال الداخلية يجب توضيحه بطرق تؤثر إيجاباً في تجارب العملاء، ولا يكون مجرد امتثال ظاهري للوائح، إذ إن عمل ما هو خلاف ذلك سيعرض المؤسسة للمخاطر. فالحوكمة الجيدة لتقنية المعلومات هي التي تتناول عمليات الأعمال الشمولية بمجملها وتقوم بتنسيق أنشطة المؤسسة مع مرور الوقت وعبر حدود المنظمة.

وكما سنرى في فصول هذا الكتاب، فإن حوكمة تقنية المعلومات لا يجب أن تُؤخذ في الاعتبار فقط عند إطلاق المؤسسة لمبادرة جديدة، ذلك أنها ليست مشروعاً يبدأ وينتهي بشكل منفصل، لكن يجب اعتبارها عنصراً أساسياً في نسيج المؤسسة يتجاوز حدود الزمن والقيادة وغيرها من المبادرات. فسواء كانت عمليات حوكمة تقنية المعلومات في المؤسسة قد تطورت بشكل غير مقصود نتيجة للعمليات التحسينية والتطويرية أو بشكل مقصود نتيجة لمشروع مدروس، فإن الأسئلة التي يجب أن يسألها المدير الأول (الأعلى) هي: إلى أي مدى كانت عمليات حوكمة تقنية المعلومات التي أجريها مفيدة في عملية تقديم قيمة للأعمال الإستراتيجية بشكل فعال عاماً بعد عام؟ وهل العمليات التي أجريها يمكن تكرارها والتنبؤ بها وتعظيمها؟ وهل هي تلبي حقاً احتياجات أعمالنا وعملائنا (بعيداً عن تبني تقنية المعلومات)؟

ومن غير المرجح أن تصلح عملية حوكمة تقنية معلومات واحدة لخدمة جميع أعمال تقنية المعلومات في المؤسسة مقارنةً بصلاحياتها لخدمة كل عميل من عملاء المؤسسة بحيث يكون راضياً تماماً عن المنتج نفسه أو عن تهيئة تقديم المنتج أو الخدمة التي تنتجها المؤسسة. ونتيجة لذلك، يلزم أن نأخذ في الاعتبار عدداً من العمليات المرتبطة بحوكمة تقنية المعلومات. إن هذه المجموعة المتكاملة من عمليات حوكمة تقنية المعلومات المتاحة هي ما نطلق عليه في فصول هذا الكتاب اسم الصورة الكاملة الكبيرة لحوكمة تقنية المعلومات (IT Governance Landscape).

إن حوكمة تقنية المعلومات ما هي إلا مجموعة جزئية من حوكمة المؤسسة، حيث تقوم وعلى أعلى مستوى بتحديد الاحتياجات التي يجب إنجازها من خلال تحسين العمليات الإدارية الشاملة. وتحيط حوكمة تقنية المعلومات ذاتياً بالنظم والبنية التحتية الشاملة لتقنية المعلومات والاتصالات. إن حوكمة تطوير منتج ما، مثل حوكمة تقنية المعلومات، تعتبر مجموعة فرعية من حوكمة المؤسسة وتتداخل مع حوكمة تقنية المعلومات. ولا تستهدف استخدام حوكمة تطوير المنتجات إلا المؤسسات التي تطور المنتجات (خلافًا لتقديم خدمة تقنية المعلومات الوارد تناولها في الفصل السابع عشر من هذا الكتاب على سبيل المثال). ولذلك ينبغي تطبيق حوكمة تطوير تقنية المعلومات في إدارات وبرامج التطوير، تلك الحوكمة التي تعتبر مجموعة فرعية من حوكمة تطوير تقنية المعلومات والمنتجات.

تقدم الفصول التالية من هذا الكتاب وتصف لنا عدة أطر ومفاهيم مهمة، بمسميات مثل كوبت (COBIT) وآيتل (ITIL)، يفهمها جيداً المتخصصون في تقنية المعلومات أكثر من المديرين التنفيذيين في المؤسسة. وعلى كل حال، فكل تلك الأمور تعتبر بمثابة أدوات وعمليات مهمة لتحسين حوكمة تقنية المعلومات في المؤسسة وتطويرها، كما سيناقش الفصل الثاني. وفي عالمنا المتمركز حول تقنية المعلومات اليوم يجب أن تدرك السلطة التنفيذية العليا في المؤسسة أهمية حوكمة تقنية المعلومات ومفاهيم أنشطة الامتثال وإدارة المخاطر المرتبطة بتقنية المعلومات. وهو ما يعتبر الهدف العام لهذا الكتاب.

۲۰

الفصل الثاني

المفاهيم الأساسية للحوكمة وقواعد قانون ساربينز أوكسلي SOx

كما ناقشنا في الفصل الأول فإن مصطلح حوكمة تقنية المعلومات المؤسسية ليس بالمصطلح الجديد، لكنه عبارة عن مفهوم له معاني مختلفة بالنسبة لأشخاص مختلفين. وقد استمر تطور مفهوم الحوكمة المؤسسية خلال السنوات الأخيرة خاصة في الولايات المتحدة. واستجابة لسلسلة من عمليات الاحتيال والإخفاقات التي كانت قد تعرضت لها المؤسسات خاصة في العقود الأخيرة من القرن الماضي، فقد كان هناك تركيز كبير على عملية تحسين مدونات قواعد السلوك في المؤسسة وإنشاء ما يسمى بإدارات أخلاقيات العمل. وقد شارك مؤلف هذا الكتاب في قضايا حوكمة الشركات عندما أوكل إليه إدارة التدقيق الداخلي في واحدة من كبرى الشركات الأمريكية، حيث طُلبَ منه أن يرأس فريق العمل ويقود الشركة للقيام بمراجعة العديد من القواعد الداخلية وإعادة صياغة مدونة القواعد السلوكية واستحداث إدارة لمتابعة أخلاقيات العمل في الشركة. وقد كان ذلك استجابة للتهديد الرئيسي الناجم عن الدعاوى القضائية جراء الاحتيال الذي طال المستهلكين. وقد تم تأسيس ممارسات قوية للحوكمة المؤسسية في تلك الشركة، رغم أن هذه الممارسات كانت تركز أكثر على العمليات التشغيلية العامة مع قليل من التركيز على نظم تقنية المعلومات وعملياتها التشغيلية.

لقد أصبحت قضايا الحوكمة المؤسسية ذات أهمية متزايدة في السنين الأولى من القرن الحالي عندما شهدت الولايات المتحدة سلسلة من الإخفاقات لكبرى الشركات والذي كان السبب الرئيسي لها بشكل عام هو الغش المحاسبي والاحتيال المالي. وكانت الشركة التي عُرفت بالسمعة السيئة في تلك الفترة هي شركة إنرون Enron التجارية. فقد كان الإخفاق المفاجئ وغير المتوقع لتلك الشركة ناتجاً عن الاحتيال المالي الذي تسبب في الزج بالعديد من المديرين التنفيذيين للشركة في السجون. وقد عَجَّلَ هذا الإخفاق لشركة إنرون في إقرار قانون ساربينز أوكسلي SOX في الولايات المتحدة الأمريكية، وكذلك في إيجاد مطالب مماثلة في جميع أنحاء العالم. ستقدم الأجزاء التالية من هذه الوحدة لمحة عامة عن الضوابط الداخلية لقانون SOx والتشريعات القانونية للحوكمة.

تسلك المفاهيم العامة للحوكمة التي ناقشناها في الفصل الأول اتجاهًا مغايرًا بعض الشيء عندما نقوم بتقديم مفاهيم ونظم تقنية المعلومات ووضعها في مزيج واحد. فالعديد من المفاهيم العامة لدينا حول حوكمة الإدارة قد تأسست واكتملت نوعاً ما في النصف الأخير من القرن العشرين. فوضعت معايير، وكذلك ممارسات العمل بين الإدارة والمدققين الخارجيين والهيئات التنظيمية.

بالإضافة إلى إعطاء لمحة عامة حول المفاهيم الخاصة بقانون SOx، فإن هذا الفصل سيقدم أيضاً عرضاً رفيع المستوى لقضايا حوكمة تقنية المعلومات، متضمناً ذلك قضايا المؤسسة التشريعية والأمنية والمخاطر المرتبطة بتقنية المعلومات. كما سيناقش هذا الفصل التهديدات الداخلية والخارجية التي تؤثر في عمليات حوكمة تقنية المعلومات المؤسسية، إضافة إلى بعض خصائص الحوكمة الفعالة لتقنية المعلومات في المؤسسة. ويستعرض هذا الفصل أيضاً كلاً من المفاهيم العامة والخاصة لحوكمة تقنية المعلومات التي تُطبق على كبار المديرين اليوم. وسيتم الرجوع إلى العديد من هذه المفاهيم لاحقاً ومناقشتها بمزيد من التفصيل في فصول أخرى.

قانون ساربنز أوكسلي SOx:

قانون SOx هو قانون أمريكي كان قد صدر عام ٢٠٠٢ لتحسين عمليات إعداد التقارير المالية والتدقيق والحوكمة المؤسسية في الشركات العامة. وقد كان لهذا القانون في البداية أثر كبير في الأعمال في الولايات المتحدة، أما الآن فقد تم الاعتراف به واعتماده في جميع أنحاء العالم. وعلى الرغم من أن قواعد التدقيق والرقابة الداخلية لهذا القانون قد أسهمت وبشكل مباشر في تغيير العديد من ممارسات التدقيق الخارجي والممارسات المالية الخاصة بتقنية المعلومات، فإنه كان لهذا القانون أثر كبير أيضاً في حوكمة تقنية المعلومات. إن الفهم العام لهذا القانون من خلال التركيز على البند ٤٠٤ والمتعلق بقواعد الرقابة المحاسبية الداخلية يعد مطلب معرفي رئيسي بالنسبة لجميع كبار المديرين.

لقد أصبح قانون SOx قانوناً أمريكياً استجابةً لسلسلة من المخالفات المحاسبية والإخفاقات المالية التي كانت قد تعرضت لها في السابق شركات كبرى كإنرون Enron وورلد كوم WorldCom. وقد تسبب قانون SOx في إحداث العديد من التغيرات

الرئيسية التي كانت قد أثرت في عمليات حوكمة الشركات والعمليات المحاسبية وعمليات تدقيق التقارير المالية -بداية في الولايات المتحدة وحالياً في جميع أنحاء العالم. وعلى الرغم من أن قانون SOx عبارة عن مجموعة شاملة من التشريعات التي تحتوي على العديد من المكونات، فإن الجزء الأعظم من اهتمام الأعمال والمدققين الخاضعين لهذا القانون قد انصب على البند ٤٠٤ منه والمتعلق بقواعد تصديق أو إقرار الخضوع للرقابة الداخلية. وقد تسببت هذه الإجراءات المتعلقة بتدقيق الرقابة الداخلية في بذل المزيد من الجهد والاهتمام عندما بدأت الشركات بإقرار الالتزام بقانون SOx. يقدم هذا القسم نظرة عامة رفيعة المستوى عن قانون SOx الموجود حالياً، مع التركيز أكثر على البند ٤٠٤ منه والقواعد الأكثر أهمية بالنسبة لقضايا حوكمة تقنية المعلومات. وسنلخص متطلبات هذا القانون الخاصة بمراجعات الضوابط المحاسبية الداخلية، كما سنلخص أحد معايير التدقيق الخارجي الذي يعتبر جديداً نسبياً والذي يطلق عليه معيار التدقيق رقم (AS5 5) Auditing Standard No. 5، وهو مجموعة إضافية من طرق الرقابة القائمة على المخاطر والذي يؤكد أيضاً أهمية القيام بمراجعات للضوابط الداخلية للتقارير المالية. بناء على ما تقدم فإنه يجب أن يكون لدى جميع كبار المديرين في المؤسسة مستوى عام من المعرفة والفهم الخاصة بقواعد الرقابة الداخلية لقانون SOx^(١).

العناصر الأساسية لحوكمة تقنية المعلومات الخاصة بقانون SOx:

إن الاسم الرسمي لقانون SOx هو قانون إصلاح المحاسبة العامة وحماية المستثمرين (Public Accounting Reform and Investor Protection Act). وقد أصبح قانوناً تشريعياً في شهر أغسطس عام ٢٠٠٢م، وتم إصدار معظم القواعد واللوائح التنظيمية التفصيلية النهائية لهذا القانون مع نهاية العام التالي. ولأن اسمه يبدو طويلاً بعض الشيء، فقد أطلق عليه رجال الأعمال اسم قانون ساربنز أوكسلي SOx نسبة لأسماء أعضاء الكونجرس الأمريكي الأساسيين الرعاة لهذا القانون. يشير أغلب المهنيين بشكل عام إلى هذا القانون باسم SOx، أو SOX، أو Sarbox، وذلك من بين العديد من الأسماء الأخرى.

لقد قدم قانون SOx مجموعة من العمليات المختلفة كلياً فيما يخص الرقابة الخارجية، كما قام بإسناد العديد من المسئوليات الجديدة للحوكمة إلى كبار المديرين التنفيذيين وأعضاء مجلس الإدارة. كما تم بموجب هذا القانون إنشاء مجلس الإشراف المحاسبي على الشركات المساهمة (Public Company Accounting Oversight Board (PCAOB وهو الهيئة المسؤولة عن وضع القوانين، وهو خاضع لهيئة الأوراق المالية والبورصة الأمريكية (Securities and Exchange Commission (SEC وهي الهيئة التي تقوم بإصدار المعايير الخاصة بالتدقيق المالي والإشراف على حوكمة المدقق الخارجي. وكما هو الحال بالنسبة لجميع القوانين الاتحادية المتعلقة بالأموال والسندات المالية، فقد تم تطوير مجموعة إضافية من اللوائح والقوانين الإدارية من قبل هيئة الأوراق المالية والبورصة الأمريكية وذلك استناداً إلى تشريعات SOx.

يتم تنظيم وإصدار القوانين الاتحادية الأمريكية على شكل أقسام منفصلة بداخل القانون التشريعي تسمى أبواب، ويندرج تحت كل باب مجموعة من البنود المرقمة والبنود الفرعية. ويشتمل قانون SOx على العديد من القواعد التي ليست بتلك الأهمية الكبيرة بالنسبة للعديد من المهنيين. نذكر على سبيل المثال البند ٦٠٢ (د) من الباب الأول والتي تنص على أنه يجب على هيئة الأوراق المالية والبورصة الأمريكية أن تضع الحد الأدنى من معايير أو قواعد السلوك المهني الخاصة بالمحامين الممارسين والتابعين للجنة مراقبة عمليات البورصة^(١). وقد يكون من الجيد أن نعرف أن هذا الأمر ليس له أي تأثير يذكر في إدارة المؤسسة وحوكمة تقنية المعلومات. يوجز الشكل التوضيحي (٢-١) الأبواب أو البنود الرئيسية لقانون SOx، علماً بأن تركيزنا سيكون فقط على الباب الأول والرابع من القانون. فلسنا بصدد وصف جميع بنود قانون SOx أو إعادة نشر النص الكامل لهذا التشريع الذي يمكن أن نجده على شبكة الويب^(٢)، وإنما نهدف إلى تسليط الضوء على الأجزاء الأكثر أهمية بالنسبة للمهنيين المعنيين بهذا القانون. وسنبداً بمناقشة الباب الأول من قانون SOx والخاص بمجلس الإشراف المحاسبي على الشركات المساهمة PCAOB وقواعد البند ٤٠٤.

^(١) وهي أحد بنود الباب السادس، وتنص على وضع قيود تحد من ممارسة المهنيين بصفة وسيط أو مستشار أو تاجر (المترجم).

شكل توضيحي (١-٢)

موجز الأحكام الرئيسية لقانون SOx.

البند	الموضوع	القاعدة أو الشرط المطلوب
١٠١	إنشاء مجلس الإشراف المحاسبي على الشركات المساهمة PCAOB.	القواعد العامة لإنشاء مجلس الإشراف المحاسبي على الشركات المساهمة PCAOB متضمنة متطلبات الحصول على عضوية المجلس.
١٠٤	مراقبة شركات المحاسبة	الجدول الزمني لعمليات التفتيش التي يقوم بها مجلس الإشراف المحاسبي على الشركات المساهمة PCAOB على شركات المحاسبة العامة المسجلة.
١٠٨	معايير التدقيق	سيقبل مجلس الإشراف المحاسبي على الشركات المساهمة PCAOB معايير التدقيق الحالية إلا أنه سيقوم بإصدار معايير جديدة له.
٢٠١	ممارسات خارج النطاق	تحدد الممارسات المحظورة على شركات المحاسبة كالاستعانة بمصدر خارجي لعملية التدقيق الداخلي (تعهد التدقيق الداخلي)، أو مسك الدفاتر المحاسبية أو تصميم النظم المالية.
٢٠٣	تناوب شريك التدقيق	يجب تبديل المدقق الرئيسي والمدقق المراجع بشكل منتظم كل خمس سنوات.
٣٠١	استقلالية لجنة التدقيق	يجب على جميع أعضاء لجنة التدقيق أن يكونوا مديرين مستقلين.
٣٠٢	مسؤولية الشركات عن التقارير المالية.	يجب أن يصدق كل من الرئيس التنفيذي CEO والمدير المالي CFO شخصياً على جميع التقارير المالية الدورية.
٣٠٥	موانع خاصة بالموظفين والمديرين	إذا تم تلقي مقابل أو مكافأة كجزء من عملية احتيالية أو عملية محاسبية غير قانونية، فإن الموظف أو المدير المستفيد مطالب بإعادة الأموال التي تلقاها بشكل شخصي.
٤٠٤	تقارير الرقابة الداخلية	الإدارة هي المسؤولة عن التقييم السنوي للضوابط الداخلية.
٤٠٧	الخبير المالي	يجب أن يكون الخبير المالي أحد مديري لجنة التدقيق.

٤٠٨	تحسين مراجعة الإفصاحات المالية.	قد تقوم هيئة الأوراق المالية والبورصة الأمريكية بوضع إطار زمني لعدة مراجعات للمعلومات المالية المدونة بالتقارير استناداً إلى عوامل محددة.
٤٠٩	الإفصاح في الوقت الحقيقي	يجب أن توزع التقارير المالية بطريقة سريعة وفورية.
١١٠٥	محظورات الموظف أو المدير	قد تمنع هيئة الأوراق المالية والبورصة الأمريكية المدير أو الموظف من العمل في شركة عامة أخرى في حال كان مدان في إحدى المخالفات.

الباب الأول من قانون SOx: مجلس الإشراف المحاسبي على الشركات المساهمة PCAOB:

قدم قانون SOx قواعد جديدة وهامة للمدققين الخارجيين. فقبل ظهور قانون SOx كان المعهد الأمريكي للمحاسبين القانونيين (AICPA (American Institute of Certified Public Accountants هو المسؤول عن وضع الإرشادات لجميع المدققين الخارجيين وشركات المحاسبة العامة التي يعملون بها وذلك من خلال مسؤوليته الكاملة عن شهادة المحاسب القانوني (CPA) Certified Public Accountant. وبينما قامت مجالس المحاسبة في الولايات في الواقع باعتماد محاسبين قانونيين CPAs، كان المعهد الأمريكي للمحاسبين القانونيين هو السَّابِق في حمل كامل المسؤولية الخاصة بالمهنة. كما تم أيضاً وضع معايير التدقيق الخارجي من قبل مجلس معايير التدقيق Auditing Standards Board (ASB) التابع للمعهد الأمريكي للمحاسبين القانونيين AICPA. وعلى الرغم من أن المعايير الأساسية - التي يطلق عليها اسم معايير التدقيق المقبولة قبولاً عاماً (GAAS) Generally Accepted Auditing Standards - كانت موجودة دائماً ومعمولاً بها على مر السنين، إلا أن هناك معايير تدقيق أحدث قد تم إصدارها على شكل نشرات مرقمة عن معايير التدقيق Statements on Auditing Standards (SASs). لقد كان الكثير من معايير التدقيق المقبولة قبولاً عاماً GAAS مجرد ممارسات جيدة للتدقيق، مثل أنه يجب أن تكون المعاملات المحاسبية مدعومة بالوثائق اللازمة، في

حين تناولت النشرات المرقمة لمعايير التدقيق SASs مجالات معينة بحاجة إلى مزيد من التوضيح أو التعريف. كالنشرة المعيارية رقم 99 99 SAS No. التي تناولت الاعتبارات المتعلقة بالعمليات الاحتيالية في القوائم المالية. حيث تشترط قواعد السلوك المهني الخاصة بالمعهد الأمريكي للمحاسبين القانونيين وجود محاسبين قانونيين (CPAs) لاتباع جميع معايير التدقيق (القابلة للتنفيذ) والتوافق معها.

وقد قامت هيئة الأوراق المالية والبورصة الأمريكية بقبول معايير التدقيق المقبولة قبولاً عاماً والخاصة بالمعهد الأمريكي للمحاسبين القانونيين (AICPA's GAAS) ونشرات معايير التدقيق SAS الخاصة بها. وقد حددت قواعد التدقيق هذه، معايير التدقيق الخارجي والاختبارات الضرورية التي يجب تطبيقها على القوائم المالية الخاضعة للتدقيق. من جهة أخرى، أشارت الفصائح المحاسبية التي أدت إلى إصدار قانون SOx إلى أن عملية إنشاء معايير التدقيق التي يقودها المعهد الأمريكي للمحاسبين القانونيين قد "عطلت". وقد انتزع قانون SOx عملية وضع معايير التدقيق هذه من المعهد الأمريكي للمحاسبين القانونيين والتي كانت خاضعة لهيمنة شركات المحاسبة العامة الكبرى، كما عمل القانون على إنشاء مجلس الإشراف المحاسبي على الشركات المساهمة، وهو مؤسسة غير اتحادية، وغير ربحية تقع على عاتقها مسؤولية الإشراف على جميع عمليات التدقيق الخاصة بالشركات التي تخضع لهيئة الأوراق المالية والبورصة الأمريكية.

إن مجلس الإشراف المحاسبي على الشركات المساهمة PCAOB ليس بديلاً عن المعهد الأمريكي للمحاسبين القانونيين AICPA، ولكنه تولى المسؤولية عن ممارسات التدقيق الخارجي التي يقوم بها الأعضاء التابعون للمعهد الأمريكي للمحاسبين القانونيين. ولا يزال المعهد الأمريكي للمحاسبين القانونيين مستمراً في إدارة اختبار المحاسب القانوني المعتمد CPA وشهادته التي تُمنح تبعاً لكل ولاية، كما يقوم المعهد أيضاً بوضع معايير التدقيق للمنظمات الأمريكية الخاصة غير الخاضعة لهيئة الأوراق المالية والبورصة الأمريكية. وبينما يحدد الباب الأول من قانون SOx ممارسات التدقيق الخاصة بمجلس الإشراف المحاسبي على الشركات المساهمة التي يقوم بها المدققون الخارجيون، نجد أن القواعد الأخرى لعمليات التدقيق وحوكمة الشركات قد أسهمت أيضاً في تغيير الكيفية التي ينسق بها المدققون

الداخليون أعمالهم مع المدققين الخارجيين. وعلى الرغم من أن الباب الأول من قانون SOx يحتوي على العديد من القواعد الجديدة، قد تكون القواعد الثلاث الأكثر أهمية بالنسبة للعديد من كبار المديرين هي أن مجلس الإشراف المحاسبي على الشركات المساهمة حالياً هو من تقع على عاتقه المسؤولية الرئيسية عن مراقبة شركات المحاسبة العامة، وهو الذي يقوم أيضاً بوضع القواعد الخاصة بمعايير التدقيق الخارجي لهذه الشركات، ويقوم كذلك بوضع قواعد معايير التدقيق كاحتفاظ بأوراق العمل. تصف الفقرات التالية بإيجاز قواعد عملية التدقيق الخارجي تلك والواردة في الباب الأول من قانون SOx.

إدارة مجلس الإشراف المحاسبي على الشركات المساهمة PCAOB وتسجيل شركات المحاسبة العامة: يدار مجلس الإشراف المحاسبي على الشركات المساهمة من خلال مجلس معين من قبل هيئة الأوراق المالية والبورصة الأمريكية بعضوية مشروطة غير خاضعة لهيمنة مصالح المحاسبين القانونيين CPA وشركات المحاسبة العامة. ويكون مجلس الإشراف المحاسبي على الشركات المساهمة هو المسؤول عن الإشراف على جميع شركات المحاسبة العامة التي كانت تمارس عملها قبل إنشاء هيئة الأوراق المالية والبورصة الأمريكية وتنظيمها، كما أنه مسئول أيضاً عن وضع معايير التدقيق.

معايير التدقيق ومراقبة الجودة والاستقلال: يمتلك مجلس الإشراف المحاسبي على الشركات المساهمة سلطة وضع معايير التدقيق والتوثيق المتعلقة بها، وكذلك معايير مراقبة الجودة وأخلاقيات العمل في شركات المحاسبة العامة المسجلة. كما يعترف قانون SOx بمعايير التدقيق التي كانت قد صدرت في السابق عن المعهد الأمريكي للمحاسبين القانونيين، وقد أصدر هذا القانون حتى الآن عدداً محدوداً من المعايير الجديدة، كمعيار التدقيق رقم 5 AS5 الخاص بمراجعة وتقييم الضوابط الداخلية. وتوضح قواعد قانون SOx أيضاً أنه يجب أن يتضمن تقييم المدقق الخارجي وصف نقاط الضعف الجوهرية وكذلك جميع الأمور الخاصة بعدم الامتثال الجوهرية التي تم الكشف عنها. فالمدققون الخارجيون مطالبون بتعديل فاعلية الضوابط الداخلية. وغياب مثل هذا التوثيق يجب اعتباره أحد نقاط الضعف في الضوابط الداخلية.

الاحتفاظ بأوراق عمل التدقيق: أوراق العمل هي الوثائق التي أعدت بواسطة المدققين خلال عملية التدقيق. ووفقاً لمعيار التدقيق رقم 3 AS3 الصادر عن مجلس الإشراف المحاسبي على الشركات المساهمة والخاص بوثائق التدقيق، فإنه يجب الاحتفاظ بأوراق العمل الخاصة بالتدقيق وغيرها من الوثائق الداعمة لفترة زمنية لا تقل عن سبع سنوات. وقد جاء هذا المطلب بالتأكيد رداً على حدث مؤسف كان قد وقع قبيل سقوط شركة إنرون ومن ثم سقوط آرثر أندرسون Arthur Andersen، وهو مكتب التدقيق الخارجي للشركة. فقد كانت شركة إنرون لا تزال تعمل، ولكنها تعاني بعض الضغوطات المالية عندما أعلنت هيئة الأوراق المالية والبورصة الأمريكية بأنها تنوي إجراء معايينة فعلية (لوثائق التدقيق). وعلى إثر ذلك قام (مدققو مكتب) آرثر أندرسون، المدقق الخارجي للشركة، باستخدام إحدى السياسات الداخلية للشركة لتبرير عملية إتلاف جميع بل معظم وثائق التدقيق الحالية الخاصة بالشركة. وكان هذا الحدث أحد العوامل المحفزة التي أدت إلى وجود هذه القاعدة في قانون SOx.

نطاق اختبار الضوابط الداخلية: تشترط مبادئ مجلس الإشراف المحاسبي على الشركات العامة وجود مدققين خارجيين يقومون بوصف نطاق كلٍّ من عمليات الاختبار ونتائجها. فقبل ظهور قانون SOx كان المدققون الخارجيون أحياناً يقومون باستخدام السياسات الداخلية للشركة لتبرير العديد من الاختبارات التي يجرونها على عينات صغيرة من العناصر، فقد جرت العادة بأن يقوموا بإجراء اختباراتهم على عينات صغيرة من الأشخاص بالرغم من وجود عدد كبير من الذين يمكن إخضاعهم لعمليات الاختبار. وعندما تظهر النتائج الإيجابية للاختبارات ولم تظهر أية مشكلات، فإنهم يقومون بتعميم تلك النتائج الخاصة بالاختبارات التي أجريت على العينة الصغيرة على جميع العناصر أو الأشخاص. أما الآن فيجب عليهم إعطاء مزيد من الاهتمام لكلٍ من نطاق ومعقولية إجراءات الاختبار لديهم، ويجب أن تصف الوثائق المساندة بوضوح نطاق ومدى أنشطة الاختبار.

الباب الرابع لقانون SOx's: الإفصاحات المالية المعززة والبند 404:

تم تخصيص الباب الرابع من قانون SOx لمعالجة بعض المشاكل الخاصة بالإفصاح عن التقارير المالية، والتشديد على القواعد الخاصة بتضارب المصالح بالنسبة لموظفي ومديري

الشركة، وتفويض الإدارة بتقييم الضوابط الداخلية، وإصدار مدونة قواعد السلوك لكبار الموظفين وغيرها من القضايا. يوجد العديد من البنود في هذا الباب، إلا أن البند الأكثر أهمية بالنسبة لمعظم كبار المديرين هو البند ٤٠٤ والذي يدور حول تقييم الإدارة للضوابط الداخلية. يشترط قانون SOX أن تحتوي جميع تقارير (10K)^(*) السنوية على تقرير الضوابط الداخلية الذي ينص على مسئولية الإدارة عن إنشاء نظام مناسب للضوابط الداخلية والحفاظ عليه، وكذلك تقييم الإدارة مدى فاعلية تلك الإجراءات الموضوعة للضوابط الداخلية، وذلك اعتباراً من تاريخ انتهاء السنة المالية. هذا ما يُعرّف عموماً بقواعد البند ٤٠٤. ويتحمل كل من المدققين الداخليين ومدققي تقنية المعلومات والاستشاريين الخارجيين وحتى الفريق الإداري - باستثناء المدققين الخارجيين - المسئولية عن مراجعة وتقييم فاعلية الضوابط الداخلية لديهم، ثم يأتي بعد ذلك دور المدققين الخارجيين للتصديق على مدى كفاية تلك المراجعات للضوابط الداخلية التي تم بناؤها ومراقبتها من قبل الإدارة.

يتم دعم عمليات المراجعة الخاصة بالبند ٤٠٤ من قبل قواعد معيار التدقيق رقم ٥ AS5 والتي ستناقش لاحقاً في هذا الفصل، وهي تعد من الأمور الهامة وخصوصاً للمدققين الداخليين نظراً لأن هذه القواعد توضح أنه من الممكن للمدققين الخارجيين أن يقوموا بعمل المدققين الداخليين في مراجعاتهم للضوابط الداخلية.

تنص قواعد البند ٤٠٤ من قانون SOX على أن المؤسسة هي المسؤولة عن مراجعة وتوثيق واختبار الضوابط المحاسبية الداخلية لديها، مع تمرير نتائج تلك المراجعات إلى المدققين الخارجيين للمؤسسة والمكلفين بمراجعة تلك الأعمال والتصديق عليها على أنها جزء من مهامهم المتعلقة بمراجعة القوائم المالية المعلن عنها. عندما تم سن قانون SOX لأول مرة، كانت عمليات المراجعة الواردة في البند ٤٠٤ هي نقطة الاهتمام الرئيسية بالنسبة للعديد من المؤسسات نظراً لأن المدققين الخارجيين كانوا في السابق يتبعون مجموعة تفصيلية للغاية من الإجراءات الخاصة بعملية تدقيق المحاسبة المالية التي تم تحديدها في معيار التدقيق رقم ٢ AS2 الخاص بمجلس الإشراف المحاسبي على الشركات المساهمة، وهو

(*) هو تقرير تطلبه هيئة الأوراق المالية والبورصة الأمريكية من الشركات للتأكد من مدى التزامها، وهو عبارة عن تقرير مالي سنوي يعد من قبل الشركة في نهاية كل سنة مالية ويجب أن يكون مصدقاً من المحاسب القانوني الخاص بالشركة. (المترجم).

الأمر الذي يحتاج إلى نهج تفصيلي للمراجعة لا يسمح بأي أخطاء أو هفوات حتى لو كانت صغيرة. وقد تغيرت بعد ذلك قواعد التدقيق الواردة في البند ٤٠٤ مع صدور معيار التدقيق رقم AS5 ٥ من مجلس الإشراف المحاسبي على الشركات المساهمة في عام ٢٠٠٧، والذي يعد أحد أساليب التدقيق القائمة أكثر على المخاطر، كما يسمح أيضاً للمدققين الخارجيين باستخدام أعمال المدققين الداخليين في إجراء التقييمات الخاصة بهم على نحو أفضل.

البند ٤٠٤ تقييمات الضوابط الداخلية:

كانت الإدارة دائماً هي التي تتحمل المسؤولية الكاملة عن تصميم وتطبيق ضوابط الرقابة الداخلية على عمليات التشغيل داخل المؤسسة. وعلى الرغم من أن معايير تكوين الضوابط الداخلية الجيدة لم تكن دائماً محددة بشكل جيد في الماضي، إلا أنها بقيت أحد المفاهيم الرئيسية للإدارة. يشترط البند ٤٠٤ من قانون SOx القيام بإعداد تقرير سنوي عن الضوابط الداخلية، يشتمل على عناصر المعلومات التالية، على أنها جزء من نموذج التقرير السنوي 10k الذي تم فرضه من قبل هيئة الأوراق المالية والبورصة الأمريكية.

- بيان رسمي من الإدارة يقر بمسؤولية المؤسسة عن إنشاء وصيانة هيكل وإجراءات مناسبة للرقابة الداخلية الخاصة بالتقارير المالية.

- تقييم لفاعلية بنية وإجراءات الرقابة الداخلية للتقارير المالية في المؤسسة، اعتباراً من نهاية آخر سنة مالية.

وبالإضافة إلى ذلك، فإن مكتب التدقيق الخارجي الذي قام بإصدار التقرير الداعم للتدقيق، مطالب هو الآخر بمراجعة تقييم الإدارة للضوابط المالية الداخلية الخاصة بها والإفصاح عن النتائج. نستطيع القول ببساطة إن الإدارة مُطالبة بالإعلان عن جودة ضوابط الرقابة الداخلية لديها، كما يجب على شركة المحاسبة العامة أن تدقق أو تصادق على أن الإدارة قد قامت فعلاً بتطوير تقرير عن الضوابط الداخلية بالإضافة إلى عملها الطبيعي والخاص بتدقيق القوائم المالية. لقد جرت العادة بأن تكون الإدارة هي المسؤولة عن إعداد تقاريرها المالية الدورية، ثم يأتي بعد ذلك دور المدققين الخارجيين الذين يقومون بتدقيق تلك الأرقام المالية والتصديق على سلامتها. فبموجب البند ٤٠٤ من قانون SOx تكون

الإدارة هي المسؤولة عن توثيق وفحص الضوابط المالية الداخلية لديها وكذلك الإفصاح عن مدى كفاءتها. ثم يقوم المدققون الخارجيون بعد ذلك بمراجعة المواد الداعمة التي نتج عنها هذا التقرير الخاص بالضوابط المالية الداخلية للتأكيد على أن هذا التقرير ما هو إلا وصف دقيق لبيئة الرقابة الداخلية.

بالنسبة لمدقق القوائم غير المالية وبالتأكيد بالنسبة للعديد من كبار مسؤولي الأعمال التنفيذيين، قد يبدو ذلك مطلباً غامضاً أو تافهاً بعض الشيء. حتى إن بعض المدققين الداخليين المنشغلين بالدرجة الأولى في عمليات التدقيق التشغيلية قد يتساءلون عن الفروقات البسيطة في هذه العملية. في جميع الأحوال، فإن تقارير التدقيق المتعلقة بحالة الضوابط الداخلية كانت نقطة خلاف مستمرة بين المدققين الخارجيين وهيئة الأوراق المالية والبورصة الأمريكية وغيرها من الأطراف المعنية على الأقل منذ عام ١٩٧٤. وكان جزء كبير من المشكلة هو عدم وجود تعريف متفق عليه يوضح المقصود بالضوابط الداخلية.

يصف إطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية Committee Of Sponsoring Organizations (COSO)، الذي ستم مناقشته في الفصل الرابع من هذا الكتاب، المعيار المعتمد لفهم الضوابط الداخلية. فبموجب البند ٤٠٤ من قانون SOX فإن الإدارة مطالبة بإعداد تقرير عن مدى ملاءمة ضوابطها الداخلية، مع تصديق المدققين الخارجيين على هذه التقارير التي أعدها الإدارة عن الضوابط الداخلية.

وتخضع هذه العملية إلى رقابة داخلية أساسية كمثال على أهمية الفصل بين المهام، لأن الشخص الذي يقوم بتطوير المعاملات لا ينبغي أن يكون هو الشخص نفسه الذي يوافق عليها. وبموجب إجراءات البند ٤٠٤، فإن المؤسسة هي التي تقوم ببناء وتوثيق عمليات الرقابة الداخلية لديها، ثم تقوم بعد ذلك جهة مستقلة كالتدقيق الداخلي بمراجعة وفحص تلك الضوابط الداخلية، وأخيراً يقوم المدققون الخارجيون بمراجعة تلك العملية والتصديق على مدى كفاءتها. وسوف تستند إجراءات التدقيق المالي الخاصة بهم إلى تلك الضوابط الداخلية. إن هذه العملية الواردة في البند ٤٠٤ تقوم بتحسين الأمور التي كانت موجودة في الأيام التي سبقت صدور قانون SOX عندما كان يقوم المدققون الخارجيون ببناء وتوثيق وتدقيق الضوابط الداخلية لديهم بشكل متكرر، وهذا يعد خلافاً في الفصل بين المهام.

تحديد العمليات الرئيسية للبدء في مراجعة الإمتثال للبند ٤٠٤:

لكل مؤسسة مجموعة من العمليات الأساسية تتعلق بدوراتها المحاسبية والتي من الطبيعي أن تُؤخذ في الاعتبار، سواء كان ذلك بالاعتماد على نظم تقنية المعلومات أو على الإجراءات اليدوية التي يتم أداؤها بصورة منتظمة، وهذه العمليات هي:

- **دورة الإيرادات:** وهي عمليات متعلقة بالمبيعات أو الإيرادات الأخرى للمؤسسة.
 - **دورة النفقات المباشرة:** هي عبارة عن نفقات المواد أو التكاليف المباشرة للإنتاج.
 - **دورة النفقات غير المباشرة:** عبارة عن تكاليف التشغيل التي لا يمكن ربطها مباشرة بالأنشطة الإنتاجية ولكنها ضرورية لعمليات تشغيل الأعمال بشكل عام.
 - **دورة الرواتب:** تشمل كل مستحقات العاملين.
 - **دورة المخزون:** بالرغم من أن المخزون سيعتبر في نهاية المطاف كنفقات إنتاجية مباشرة، فإن هناك حاجة لعمليات زمنية للحفاظ على المخزون لحين دخوله في الإنتاج.
 - **دورة الأصول الثابتة:** تحتاج الممتلكات والمعدات إلى عمليات محاسبية منفصلة، مثل (المحاسبة الدورية للإهلاك) بمرور الزمن.
 - **دورة الضوابط العامة لتقنية المعلومات:** تشمل هذه المجموعة من العمليات ضوابط تقنية المعلومات العامة أو القابلة للتطبيق على جميع عمليات تشغيل تقنية المعلومات.
- يعد تحديد تلك العمليات المؤسسية الرئيسية خطوة مبدئية نحو تحقيق الامتثال للبند ٤٠٤، لذلك يجب على المؤسسة أن توثق وتعي وتختبر كل تلك "العمليات الرئيسية". وبالنسبة للعديد من المؤسسات، فهذه هي النظم الرئيسية وعمليات تقنية المعلومات الداعمة لها التي تراجع سنوياً من خلال عمليات التدقيق الخارجي.

دور التدقيق الداخلي:

على الرغم من أن قانون SOx لم يعط مسؤوليات محددة لعمليات التدقيق الداخلي، فإنها تعد مصدراً هاماً لإتمام عمليات تقييم الضوابط الداخلية الواردة في البند ٤٠٤. بموجب قانون SOx، فإنه يوجد إدارة مستقلة ومنفصلة في المؤسسة - تكون إدارة التدقيق الداخلي

أو تدقيق تقنية المعلومات غالباً - تقوم بمراجعة وتوثيق الضوابط الداخلية التي تغطي العمليات الرئيسية، وتحدد نقاط الرقابة الرئيسية، وتقوم بعد ذلك باختبار هذه الضوابط المحددة. ومن ثم تقوم عملية التدقيق الخارجي بمراجعة هذا العمل وتصادق على مدى كفايته. وبالنسبة للعديد من المؤسسات، يمكن اعتبار عملية تدقيق تقنية المعلومات بأنها أحد المصادر الرئيسية لإجراء تلك المراجعات الخاصة بالضوابط الداخلية بالنسبة للعمليات القائمة على التقنية.

يجب أن تعمل الإدارة المالية العليا ولجنة التدقيق مع المدققين الخارجيين للمؤسسة لتحديد المسؤوليات الخاصة بمراجعات الضوابط الداخلية الخاصة بهم والواردة في البند ٤٠٤. وتجري هذه المراجعات سنوياً باستخدام الوثائق التي تم إعدادها واختبارها في أول سنة مالية، ثم تُحدَّث بعد ذلك ويعاد اختبارها في فترات لاحقة. لذا يجب على جميع الأطراف تطوير نهج فعال من حيث التكلفة لتحقيق متطلبات قانون SOx وتقييم تطبيقات وضوابط تقنية المعلومات لديهم.

يجب تخطيط وإجراء المراجعات الخاصة بالبند ٤٠٤ من قانون SOx على غرار العديد من المشاريع الجديدة في تقنية المعلومات، كما جاء في الفصل التاسع عشر الذي يدور حول دور التدقيق الداخلي في حوكمة تقنية المعلومات. الشكل التوضيحي (٢-٢) يوجز بعض اعتبارات التخطيط اللازمة لمراجعة الرقابة الداخلية الواردة في البند ٤٠٤ على أن يتم تنفيذها من قبل المدققين الداخليين في المؤسسة، والذين بإمكانهم أن يلعبوا دوراً أساسياً في مساعدة الإدارة العليا على تحقيق الامتثال مع ما ورد في البند ٤٠٤. نحن لا نهدف هنا إلى توفير إرشادات للتدقيق الداخلي بقدر ما نهدف إلى إعطاء المدير الأول (الأعلى) فكرة عن تلك العمليات الخاصة بالتدقيق الداخلي لتقنية المعلومات.

شكل توضيحي (٢-٢)

اعتبارات التخطيط لمراجعة الضوابط الداخلية الواردة في البند ٤٠٤

١.	حدد حالة المراجعة - هل هذه هي الجولة الأولى من المراجعات الواردة في البند ٤٠٤ بالنسبة للمؤسسة وسيتم متابعتها في السنوات اللاحقة؟
٢.	إذا كانت هذه هي المراجعة الأولى (مراجعة جديدة) اتبع خطوات العمل اللازمة لفهم وتوثيق واختبار العمليات الرئيسية. خلاف ذلك، خطط للمراجعة في فترة لاحقة.
٣.	قم بمراجعة الوثائق التفصيلية للمراجعات السابقة للبند ٤٠٤، متضمناً ذلك خرائط تدفق الإجراءات، وفجوات الرقابة الداخلية التي تم تحديدها ومعالجتها، وكذلك الوثائق الشاملة لتخطيط المشروع والخاصة بالمراجعة السابقة.
٤.	قم بمراجعة أي من القواعد الصادرة عن مجلس الإشراف المحاسبي على الشركات المساهمة قد تم نشرها مؤخراً يمكن أن تغطي المراجعات الواردة بالبند ٤٠٤ وتتعلق بالتغيرات التي تطرأ على التدقيق، وقم بضبط إجراءات المراجعة بحيث تعكس تلك التغيرات.
٥.	قم بالاجتماع مع مكتب التدقيق الخارجي المسئول عن التصديقات الحالية للبند ٤٠٤ وقم بتحديد ما إذا كان هناك أي تغيرات في الوثائق وفلسفة الاختبار، مع التأكيد على قواعد معيار التدقيق رقم AS5 ٥، من تلك المراجعة السابقة.
٦.	ضع في الاعتبار أي تغيرات تنظيمية قد طرأت منذ المراجعة السابقة، متضمناً ذلك الاستحواذات أو العمليات الرئيسية لإعادة الهيكلة، وتعديل المدى الذي ستقوم المراجعة بتغطيته، إذا اقتضت الحاجة ذلك.
٧.	من خلال اللقاءات مع الإدارة العليا وإدارة تقنية المعلومات، حدد ما إذا كان هناك نظم وعمليات جديدة قد تم تنصيبها خلال الفترة الماضية، وإذا ما كانت هذه التغيرات الجديدة قد تم تدوينها في الوثائق المحدثة.
٨.	قم بمراجعة أي من نقاط الضعف الخاصة بالرقابة الداخلية قد تم تعريفها في المراجعات السابقة وقم بتقييم ما إذا كانت إجراءات تصحيح الرقابة الداخلية المدونة بالتقرير يتم العمل بها على أرض الواقع.
٩.	قم بتقييم حالة الوثيقة الحالية للبند ٤٠٤ وحدد مدى ضرورة إعداد وثيقة جديدة.
١٠.	على افتراض أن المراجعة السابقة للبند ٤٠٤ قد تمت من قبل التدقيق الداخلي، قم بتحديد العناصر المدربة وذوي المعرفة المناسبة والمتاحة لإجراء المراجعة القادمة.

١١.	قم بعمل مقابلات شخصية مع جميع الأطراف التي شاركت في إجراء المراجعة السابقة للبند ٤٠٤ لتقييم أي دروس مستفادة، وقم بوضع خطط للإجراءات التصحيحية في المراجعة القادمة.
١٢.	استناداً إلى المناقشة التي تتم مع المدققين الخارجيين والإدارة العليا، قم بتحديد نطاق المعاملات الجوهرية للمراجعة القادمة.
١٣.	قم بتحديد ما إذا كانت البرمجيات - إن وجدت - المستخدمة في المراجعة السابقة لا تزال موجودة، وقم بعمل أي تغييرات ضرورية حتى يكون لديك الأدوات الكافية والجاهزة لإجراء المراجعة القادمة.
١٤.	قم بإعداد خطة تفصيلية لمشروع المراجعة القادمة للبند ٤٠٤، في ظل وجود اعتبارات معينة لتنسيق أنشطة المراجعة لدى وحدات الأعمال في المؤسسة والمدققين الخارجيين.
١٥.	قم بإرسال الخطة للموافقة عليها من قبل الإدارة العليا.

قواعد معيار التدقيق رقم ٥ AS5 والتدقيق الداخلي:

بعد فترة وجيزة من إقرار قانون SOx في الولايات المتحدة، أصدر مجلس الإشراف المحاسبي على الشركات المساهمة إرشادات معيار التدقيق رقم ٢ AS2 والذي دُعي فيه المدققون الخارجيون إلى اتباع أساليب محافظة وتفصيلية للغاية في تدقيقاتهم للقوائم المالية. فقد شدد معيار التدقيق رقم ٢ AS2 على نهج التدقيق التفصيلي (انظر في كل شيء)، وأصبحت فواتير عملية التدقيق الخارجي أغلى بكثير مما كانت عليه في السنوات الأولى لإصدار قانون SOx فضلاً عن ذلك، فقد كانت هناك شكاوى متكررة من قبل قادة الصناعة وآخرين وكان هناك إجماع عام على أن معيار التدقيق رقم ٢ AS2 يحتاج إلى بعض التنقيحات. وقد تم الاتفاق بين كل من هيئة الأوراق المالية والبورصة الأمريكية ومجلس الإشراف المحاسبي على الشركات المساهمة على تنقيح معيار التدقيق رقم ٢ AS2، وتم إصدار معيار التدقيق رقم ٥ في أواخر شهر مايو من عام ٢٠٠٧م.

معيار التدقيق رقم ٥ AS5 هو مجموعة من المعايير الخاصة بالمدققين الخارجيين الذين يقومون بمراجعة واعتماد القوائم المالية المنشورة. وتعتبر هذه القواعد مهمة أيضاً بالنسبة للمدققين الداخليين. يقدم معيار التدقيق رقم ٥ مجموعة من القواعد القائمة على المخاطر مع التركيز على كفاءة الضوابط الداخلية المعتمدة أكثر على أحداث وظروف المؤسسة. هذا

بالإضافة إلى أن معيار التدقيق رقم ٥ يدعو المدققين الخارجيين أن يأخذوا بعين الاعتبار جميع مراجعات التقارير المناسبة الخاصة بالتدقيق الداخلي أثناء مراجعاتهم المتعلقة بتدقيق القوائم المالية. حيث يسمح هذا المعيار للمدققين الخارجيين بأن يركزوا أكثر على قدرة الإدارة على إيجاد وتوثيق الضوابط الداخلية الرئيسية.

إن لقواعد معيار التدقيق رقم ٥ أهمية خاصة بالنسبة للمدققين الداخليين نظراً لإمكانية اعتماد المدققين الخارجيين على أعمال المدققين الداخليين في تقييماتهم وفقاً للبند ٤٠٤. لمعيار التدقيق رقم ٥ ثلاثة أهداف رئيسية هي:

١- **تركيز عمليات تدقيق الرقابة الداخلية على المسائل الأكثر أهمية:** يدعو معيار التدقيق رقم ٥ المدققين الخارجيين إلى أن يركزوا في مراجعاتهم على المجالات ذات المخاطر البالغة التي ستعجز الرقابة الداخلية عن منع أو اكتشاف التقارير غير الواضحة في البيانات المالية. إن هذا النهج يدعو المدققين الخارجيين أن يركزوا على تحديد نقاط الضعف الجوهرية في الرقابة الداخلية أثناء مراجعاتهم قبل أن تتسبب في وقوع أخطاء جسيمة في البيانات المالية. ويشدد معيار التدقيق رقم ٥ أيضاً على أهمية تدقيق المجالات العالية المخاطر، مثل عملية إقفال نهاية الفترة للقوائم المالية والضوابط المصممة لمنع الاحتيال من قبل الإدارة. وفي ذات الوقت يوفر هذا المعيار مجموعة واسعة من البدائل للمدققين الخارجيين لمعالجة المجالات المنخفضة المخاطر، كأن يكون ذلك عن طريق عرض أكثر وضوحاً لكيفية التدرج في توضيح طبيعة وتوقيت ومدى الاختبار اعتماداً على المخاطر، وكذلك كيف يتم تضمين المعرفة المتراكمة من عمليات التدقيق التي تمت في السنوات السابقة في تقييم المدققين للمخاطر. وأيضاً من المهم جداً بالنسبة للمدققين الداخليين، أن معيار التدقيق رقم ٥ يسمح للمدققين الخارجيين باستخدام الأعمال التي تم تنفيذها من قبل المدققين الداخليين في المؤسسة عند الحاجة.

٢- **إزالة إجراءات التدقيق غير الضرورية لتحقيق المنافع المرجوة:** لا يشتمل معيار التدقيق رقم ٥ على المتطلبات التفصيلية التي كانت موجودة في معيار التدقيق رقم ٢ AS2 السابق لتقييم عملية التقييم الخاصة بالإدارة ولتوضيح أن عملية تدقيق الرقابة الداخلية لا تستلزم المشورة حول مدى كفاية وملاءمة عمليات الإدارة. على سبيل المثال،

يركز معيار التدقيق رقم ٥ على أبعاد المخاطر المترتبة على تعدد المواقع في المؤسسة ويقلل من المتطلبات التي تستوجب على المدققين الخارجيين بأن يقوموا بمراجعة "جزء كبير" من عمليات التشغيل أو الأوضاع المالية في المؤسسة. هذا من شأنه أن يسمح بتقليص أعمال التدقيق المالي.

٣- توسيع نطاق عملية التدقيق المالي بشكل واضح لتلائم مع حجم ومستوى التعقيد لأي مؤسسة: لتقديم الإرشادات الخاصة بعمليات التدقيق في المؤسسات الأصغر حجماً والأقل تعقيداً، يدعو معيار التدقيق رقم ٥ إلى ضبط عمليات تدقيق الضوابط الداخلية بحيث تتناسب مع حجم ودرجة تعقيد المؤسسة التي يتم تدقيقها. فلهذا المعيار إرشادات تتعلق بالكيفية التي يتم فيها تطبيق معيار التدقيق رقم ٥ على المؤسسات الأصغر حجماً والأقل تعقيداً وكذلك على وحدات المؤسسات الأكبر حجماً.

عقب إصدار معيار التدقيق رقم ٥ ، قد يفكر المدققون الخارجيون في مسألة استخدام أعمال الآخرين للمساعدة في إتمام تدقيق الضوابط الداخلية للقوائم المالية طبقاً لقانون SOx. وعلى الرغم من أن ذلك الأمر لم يكن واضحاً كما يجب وفقاً لقواعد معيار التدقيق رقم ٢ AS2 لقانون SOx، فإن معيار التدقيق رقم ٥ قد سمح بذلك الآن بشكل صريح. ينص معيار التدقيق رقم ٥ على أنه بإمكان المدقق الخارجي أن يستخدم الأعمال المنجزة بواسطة، أو أن يتلقى مساعدة مباشرة من، المدققين الداخليين أو الموظفين الآخرين في الشركة أو الأطراف الخارجية التي تعمل تحت إشراف الإدارة أو لجنة التدقيق، وذلك لتقديم الأدلة الكافية على فاعلية الضوابط الداخلية للتقارير المالية. وقد كان ذلك تغييراً جوهرياً بالنسبة للمدققين الداخليين.

من المؤكد أن المدققين الخارجيين هم من يقومون بالتوقيع أو التصديق على نتائج التدقيق، ويجب عليهم أيضاً تقدير مدى كفاءة وموضوعية الأشخاص الذين يتم التخطيط لاستخدام أعمالهم من قبل المدققين الخارجيين. فكلما زادت درجة الكفاءة والموضوعية لدى هؤلاء الأشخاص، زاد حجم الاستخدام الذي يمكن أن يفعله المدقق بأعمالهم. على وجه التحديد، يدعو معيار التدقيق رقم ٥ إلى تقييم كفاءة وموضوعية المدققين الداخليين في المؤسسة. الكفاءة هنا تعني تحقيق (والحفاظ على) مستوى معين من الفهم والمعرفة

بما يُمكن الأشخاص من أداء المهام الموكلة إليهم، أما الموضوعية فتعني المقدرة على أداء تلك المهام بنزاهة وأمانة معرفية. ولتقييم الكفاءة يتعين على المدقق الخارجي أن يقوم بتقييم مؤهلات المدققين الداخليين أو غيرهم وقدرتهم على إنجاز الأعمال التي يخطط المدقق الخارجي لاستخدامها. ولتقييم الموضوعية، فإن معيار التدقيق رقم 5 يدعو المدقق الخارجي إلى تقييم ما إذا كانت العوامل الحالية تعرقل أو تعزز من قدرة الشخص على أداء الأعمال، بالقدر اللازم من الموضوعية، والتي يخطط المدقق (الخارجي) لاستخدامها.

يوصل معيار التدقيق رقم 5 في النص على أنه لا يجب على المدققين الخارجيين استخدام أعمال أشخاص (هم) على "درجة منخفضة من الموضوعية، بغض النظر عن مستوى كفاءتهم"، كما لا يجب عليهم أيضاً استخدام أعمال أشخاص (هم) على درجة منخفضة من الكفاءة، بغض النظر عن درجة موضوعيتهم. إن الأشخاص الذين يضطلعون بمهام رئيسية كسلطة الاختبار أو الامتثال في المؤسسة، مثل المدققين الداخليين أو مدققي تقنية المعلومات، هم عادة من يُتَوَقَّع أن يكونوا على درجة عالية من الكفاءة والموضوعية في أداء مثل هذا النوع من الأعمال التي ستكون مفيدة للمدقق الخارجي.

قواعد أخرى لقانون SOX — الباب الثاني: استقلالية المدقق:

كان المدققون الداخليون والخارجيون دائماً عبارة عن موارد منفصلة ومستقلة. فقد كان المدققون الخارجيون مسؤولين عن تقييم نزاهة أنظمة الرقابة الداخلية في المؤسسة والتقارير المالية المعلنة في النهاية. في حين كان المدققون الداخليون يخدمون الإدارة في مجموعة واسعة من المجالات الأخرى. في بدايات التسعينيات من القرن الماضي، بدأ هذا الانقسام بالتغير مع تحمل شركات التدقيق الخارجي كامل المسؤولية تجاه بعض مهام التدقيق الداخلي أيضاً. وقد بدأ ذلك عندما شرعت المؤسسات الكبيرة في الاستعانة بمصادر خارجية للقيام ببعض الوظائف غير الأساسية لديها كوظيفة عامل الكفترية أو عمال الخدمات المعاونة كالنظافة والحراسة وصيانة المعدات. كان التفكير وقتها في أن الموظفين الذين عملوا في تلك المجالات المتخصصة لم يكونوا في الواقع جزءاً من عمليات التشغيل الرئيسية في المؤسسة، وأن وظيفة الخدمات المعاونة وغيرها من الوظائف غير الرئيسية الخاصة بالمؤسسة ربما يتم إسنادها إلى شركات أخرى متخصصة في مجالات مثل تقديم الخدمات المعاونة إلى العديد من المؤسسات

الأخرى. وأن موظفي الخدمات المعاونة الذين كانوا يعملون سابقاً داخل المنشأة سيتم تحويلهم إلى شركات تعمل في مجال الخدمات المعاونة، ونظرياً، فإن الكل سيستفيد. وإن المؤسسة التي بادرت بالاستعانة بالمصادر الخارجية ستتحمل تكاليف أقل، وذلك من خلال إسناد الوظيفة غير الرئيسية، وهي الخدمات المعاونة، إلى شخص ما أكثر تخصصاً فيها. وقد يكون لدى عامل الخدمات المعاونة الذي تم الاستعانة به على أنه مصدر خارجي احتمالات مهنية واعدة وإشرافية أفضل.

بدأت عملية الاستعانة بمصادر خارجية للقيام بمهمة التدقيق الداخلي لأول مرة في أواخر الثمانينيات من القرن الماضي. فقد لجأت مكاتب التدقيق الخارجي إلى إدارات الشركات التي تتولى مهام التدقيق الخارجي لديها وعرضت عليهم فكرة "الاستعانة بمصادر خارجية" أو أن تقوم الشركة بتولي المهام الحالية للتدقيق الداخلي. وقد نالت هذه الفكرة استحسان الإدارة العليا ولجان التدقيق على مختلف المستويات. حيث كانت الإدارة العليا في أغلب الأحيان غير مدركة تماماً للفروقات الموجودة ما بين مهام عملية التدقيق الخارجي والداخلي وكانوا في بعض الأحيان يميلون أكثر للتعامل مع مدققيهم الخارجيين. هذا بالإضافة إلى أن الإدارة العليا وأعضاء لجنة التدقيق كان يتم إغراؤهم غالباً عن طريق وعود بانخفاض التكاليف في حال الاستعانة بمصادر خارجية للقيام بعملية التدقيق الداخلي. وقد استمر إسناد التدقيق الداخلي لمصادر خارجية (التعهد بالتدقيق الداخلي) في النمو خلال تسعينيات القرن الماضي. وبالرغم من المحاولات المبذولة من بعض الشركات المستقلة لدخول هذا السوق، فإن إسناد التدقيق الداخلي لمصادر خارجية استمر ليكون المجال الخاص بشركات المحاسبة العامة الكبرى.

أصبحت الاستعانة بمصادر خارجية للتدقيق الداخلي مسألة بالغة الأهمية نظراً لظهوره في فضيحة إنرون، فقد قامت الشركة بتعهد مهام التدقيق الداخلي لديها بشكل شبه كلي إلى مكتب التدقيق الخارجي الخاص بها، وهو مكتب آرثر أندرسون Aruther Andersen. حيث إن فريق التدقيق، كلاهما يعمل بشكل رسمي بصفة موظف في مكتب أندرسون مع اختلاف العلاقات الخاصة بإعداد وتقديم التقارير، فهم يعملون جنباً إلى جنب في مكاتب شركة إنرون. وعلى إثر سقوط شركة إنرون، ثارت العديد من التساؤلات عقب تلك الواقعة

عن كيف يمكن لإدارة التدقيق الداخلي تلك والتي تم التعهيد بها أن تكون إدارة مستقلة عن مكتب أندرسون. لقد كان من الصعب جداً في هذه الظروف التي يمر بها التدقيق الداخلي أن تُثار المخاوف لدى لجنة التدقيق المتعلقة بمدققيهم الخارجيين. وقد أصبح هذا التضارب المحتمل بمثابة قضية إصلاحية في قانون SOx.

القيود المفروضة على خدمات المدققين الخارجيين:

نص قانون SOx على أنه من غير القانوني بالنسبة لأي شركة من شركات المحاسبة القانونية (العامة) المسجلة أن تقوم بتقديم خدمات غير متعلقة بالتدقيق بالتزامن مع تقديم خدمات التدقيق لنفس العميل. تشمل هذه المحظورات أعمال التدقيق الداخلي، والعديد من مجالات الاستشارات، والتخطيط المالي لمسئول كبير. والعنصر الأكثر أهمية هنا هو أنه من غير القانوني بالنسبة لشركات المحاسبة القانونية أن تقوم بتقديم خدمات التعهيد الخارجي لأعمال التدقيق الداخلي في حال كانت هي أيضاً من يقوم بأعمال التدقيق. هذا يعني أن شركات المحاسبة القانونية الكبرى قد تكون حالياً وبشكل أساسي خارج نطاق التعهيد الخارجي لأعمال التدقيق الداخلي بالنسبة لعملاء التدقيق المباشرين لديها. أما الشركات الأخرى، متضمناً الشركات المستقلة المنفصلة عن شركات مستوى المحاسبة العامة أو الشركات الاستشارية المتخصصة في التدقيق الداخلي يمكنهم الاستمرار في تقديم خدمات التعهيد الخارجي لأعمال التدقيق الداخلي. أما العصر الذي كان فيه من الممكن أن يصبح أحد أخصائيي التدقيق الداخلي متعاقداً أو موظفاً في شركة المحاسبة العامة الخاصة به أو بها قد انتهى.

إضافة إلى الحظر المفروض على تقديم خدمات التعهيد الخارجي لأعمال التدقيق الداخلي، فإن قانون SOx يمنع مكاتب المحاسبة القانونية من تقديم خدمات أخرى منها:

- تصميم نظم المعلومات المالية وتطبيقاتها: كانت مكاتب المحاسبة القانونية ولسنوات عديدة تقوم بتثبيت نظم مالية - تكون غالباً من تصميمها الخاص - لعملائها من الشركات. ثم يعودون بعد ذلك لمراجعة الضوابط الداخلية لتلك النظم التي قاموا للتو بتركيبها - ويعد هذا تضارباً كبيراً في المصالح، ولم يعد هذا مسموحاً به.

- **مسك الدفتر والخدمات المتعلقة بالقوائم المالية:** كانت مكاتب المحاسبة العامة في السابق تقوم بتقديم خدمات محاسبية لعملائها بالإضافة إلى قيامها بأعمال التدقيق وحتى بالنسبة للشركات الكبرى، فلم يكن من غير المعتاد بالنسبة للفريق المسئول عن عملية تدقيق القوائم المالية بالكامل أن يقوم أيضاً بإجراء الكثير من الأعمال اللازمة لبناء القوائم المالية الموحدة (المجمعة) النهائية. مرةً أخرى يعد هذا تضارباً محتملاً في المصالح، وهذا غير مسموح به.

- **الوظائف الإدارية ووظائف الموارد البشرية:** قبل صدور قانون SOX، كانت مكاتب التدقيق الخارجي هي التي تقوم غالباً باختيار عدد من المهنيين العاملين لديها وتساعد في انتقالهم إلى مناصب إدارية لدى العميل. وكانت النتيجة إيجاد بيئة يكون فيها كل مديري الحسابات تقريباً في المؤسسة هم من خريجي مكتب التدقيق الخارجي التابعين له. وقد كان ذلك محبطاً أحياناً بالنسبة للمدققين الداخليين وغيرهم من الذين لا ينتمون لمكتب المحاسبة القانونية نفسه. وبدأت فرص الحصول على ترقية فوق مستوى معين محدودة بسبب شبكة علاقات أو اتصالات "التلميذ السابق" ("Old-boy" مع مكتب التدقيق الخارجي).

- **خدمات أخرى محظورة:** يَمنع قانون SOX مكاتب التدقيق الخارجي بصورة خاصة من تقديم الخدمات الاكتوارية (المتعلقة بحسابات التأمين) والخدمات الاستشارية المتعلقة بالاستثمار والخدمات القانونية ذات الصلة بتدقيق الحسابات. بالرغم من السماح لهم بتقديم الخدمات الضريبية.

إن الموضوع العام لقانون SOX هنا هو أن المدققين الخارجيين مخولون لمراجعة القوائم المالية الخاصة بعملائهم من المؤسسات، وهذا كل ما في الموضوع. يسمح قانون SOX بتجاوز الأنشطة المحظورة التي تم ذكرها، حيث يمكن للمدققين الخارجيين المشاركة في تقديم الخدمات الأخرى غير المتعلقة بالتدقيق فحسب إذا كانت هناك موافقة مسبقة من قبل لجنة التدقيق على تقديم تلك الخدمات. فمع الفحوصات المتزايدة التي تقوم بها لجان التدقيق في ظل قانون SOX، أصبح العديد يشعرون بالقلق جراء محاولة مصادقة أي شيء يبدو أنه خارج عن المألوف إطلاقاً.

(*) العلاقات والروابط الاجتماعية والتجارية بين التلاميذ السابقين. (المترجم).

الموافقة المسبقة من لجنة التدقيق على الخدمات:

يوضح البند ٢٠٢ من الباب الأول لقانون SOx أنه يجب أن توافق لجنة التدقيق على جميع الخدمات المتعلقة وغير المتعلقة بالتدقيق بشكل مسبق. وعلى الرغم من أن لجان التدقيق كانت تفعل أو كان يجب عليها أن تفعل ذلك طيلة الوقت، فإن تلك التصديقات أو الموافقات كانت في كثير من الأحيان أكثر بقليل من مجرد إجراء شكلي، وذلك قبل صدور قانون SOx. فقد كانت لجان التدقيق في شبكة "التلاميذ السابقين" Old-Boys تتلقى غالباً ما هو أكثر قليلاً من مجرد مذكرة مختصرة مكتوبة أو رسالة شفوية من الإدارة المسؤولة عن التدقيق والتي كانت تُعتمد بالطريقة التقليدية نفسها التي كانت تُعتمد بها في كثير من الأحيان محاضر الاجتماعات. وجاء قانون SOx ليغير كل هذا، فالآن قد يُعرض أعضاء لجنة التدقيق أنفسهم للمساءلة القانونية أو إقامة دعاوى قضائية ضدهم من قبل أصحاب المصالح في حال سماحهم بحدوث أي عمل من الأعمال المحظورة.

بالطبع فإن هناك العديد من الأمور الثانوية المتعلقة بأنشطة المدققين الخارجيين التي ليس من الضروري أن تمر من خلال تلك العملية الرسمية والخاصة بالموافقة المسبقة من قبل لجنة التدقيق.

وباستخدام المصطلحات القانونية، فإن قانون SOx يضع الحد الأدنى لقواعد الاستثناء^(٣) من متطلبات الحصول على إذن لجنة التدقيق. فوفقاً لقانون SOx فإن الموافقة المسبقة ليست ضرورية بالنسبة لبعض الخدمات التي لا تتعلق بالتدقيق إذا كان:

- القيمة الإجمالية بالدولار الأمريكي للخدمة المقدمة لا تتجاوز ٥% من إجمالي رسوم عملية التدقيق الخارجي المدفوعة من قبل الشركة خلال السنة المالية التي قدمت فيها تلك الخدمات.

- كانت الخدمات المقدمة غير متعارف على أنها خدمات تتعلق بالتدقيق من قبل الشركة في الوقت الذي بدأت فيه عملية التدقيق الشامل.

- إذا حوّلت هذه الخدمات لعناية لجنة التدقيق وتم الموافقة عليها قبل إتمام عملية التدقيق.

قدّمت تلك الاستثناءات بعض المرونة للمدققين الخارجيين ولجنة التدقيق. فضلاً عن أن طبيعة ومجموع القيمة الدولارية لهذه الخدمات الإضافية التي لا تتعلق بالتدقيق يجب متابعتها بعناية طوال السنة المالية للحفاظ على مستوى معين من الامتثال. ولا بد من إشراك التدقيق الداخلي في هذه العملية للمساعدة في التأكد من أن جميع الخدمات الإضافية المقدمة لا تزال متوافقة مع قواعد قانون SOX، متضمناً ذلك الإفصاح عنها للمستثمرين عن طريق البيان السنوي للوكيل. ويسمح SOX بإمكانية أن تقوم لجنة التدقيق بتفويض سلطة الموافقة المسبقة على الخدمات التي لا تتعلق بالتدقيق لواحد أو أكثر من المديرين الخارجيين في لجنة التدقيق. وهذا من شأنه تخفيف الإجهاد الناتج عن الإجراءات المطولة للجنة التدقيق، ولكنه سيضع مسؤولية أكبر على عاتق عدد قليل من أعضاء لجنة التدقيق علاوة على العديد من المسؤوليات القانونية الجديدة المفروضة من قبل قانون SOX.

تناوب شريك التدقيق الخارجي:

صرح بند آخر (البند ٢٠٣) من الباب الثاني لقانون SOX أنه من غير القانوني أن يرأس الشريك الرئيسي لمكتب المحاسبة القانونية أية اتفاقيات لأكثر من خمس سنوات. وهي المسألة التي قامت مكاتب المحاسبة الكبرى بتصحيحها بشكل جيد قبل صدور قانون SOX. فقد كان يتم تناوب الشركاء الرئيسيين التابعين للشركات الكبرى بصفة منتظمة، على الرغم من أنه قد تكون هناك استثناءات بالنسبة للشركات الصغرى واتفاقيات الشراكة الأصغر حجماً. وفي الوقت الذي شاعت فيه عملية تناوب الشريك الرئيسي، فقد اعتبر قانون SOX أن تقصير الشركة في عملية التناوب يعد عملاً إجرامياً. فضلاً عن أن، قانون SOX في الواقع لم يتناول ممارسة عامة يتم من خلالها تناوب شريك التدقيق حيث سيقوم شخص معين بلعب دور الرئيس أو الشريك الرئيسي لعملية التدقيق، ثم يستمر بعد ذلك في الخدمة كاستشاري بعد انتهاء مدته أو مدتها. ويمكن لهذا الشريك الذي يلعب دور الاستشاري غالباً أن يحافظ على مستوى المسؤولية نفسه المعين عليه الشريك الرئيسي وقد يصبح ذلك انتهاكاً محتملاً لقواعد قانون SOX.

عند طباعة هذا الكتاب كانت هناك العديد من الشائعات والأقاويل التي تشير إلى أن مجلس الإشراف المحاسبي على الشركات المساهمة PCAOB يقوم بدراسة فرض تناوب

كامل لمكاتب المحاسبة القانونية (ليس تناوب شريكها). ففي الوقت الحالي قد يتم تبديل الشركاء ولكن يبقى المكتب دون تغيير. التفكير في أن يكون هناك مكتب جديد يمد إدارة المؤسسة بمنظور جديد حول عملية التدقيق.

يتواصل المدققون الخارجيون دائماً مع لجان التدقيق التابعين لها بصفة منتظمة طوال عملية التدقيق، وكذلك في حالة المسائل التي تثير المخاوف. وفي أعقاب سقوط شركة إنرون وغيرها من فضائح الشركات في ذلك الوقت، تم اكتشاف أن هذه الاتصالات كانت في بعض الأحيان محدودة للغاية. فقد يتفاوض أحد أعضاء الإدارة مع شريك المحاسبة القانونية على "التغاضي عن" تغيير مقترح في إحدى المعالجات المحاسبية، إلا أن لجنة التدقيق لم تكن تُبلِّغ بهذا الأمر إلا في ظل الشروط العامة، وهذا في حال حدوث ذلك.

لقد غير قانون SOx ذلك. فالمدققون الخارجيون مطالبون بالإبلاغ -على أساس زمني- عن كل السياسات والممارسات المحاسبية المستخدمة، والمعالجات البديلة للمعلومات المالية التي تمت مناقشتها مع الإدارة، والمعالجات البديلة الممكنة، والنهج الذي يفضلها المدقق الخارجي. فالفكرة كلها هنا هي أنه يجب على المدققين الخارجيين أن يقوموا بإبلاغ لجنة التدقيق التابعين لها بأي معالجات محاسبية بديلة، والنهج المفضل لدى المدققين الخارجيين، ونهج الإدارة. هذا في الواقع يقول إنه إذا كانت هناك معالجات محاسبية مختلف عليها، فإنه يجب أن تكون لجنة التدقيق على دراية جيدة بالإجراءات المتخذة حيال ذلك. ويشير هذا المطلب حقيقة إلى الحاجة إلى توثيق جيد للجنة التدقيق.

تضارب المصالح والتناوب الإلزامي لمكاتب التدقيق الخارجي:

لقد كان شائعاً في السابق بالنسبة لأعضاء فريق مكتب التدقيق الخارجي أن يحصلوا على تعيينات وظيفية لشغل مراكز مالية عليا لدى الشركات العميلة لديهم. وقد منع البند ٢٠٦ من الباب الثاني لقانون SOx المدققين الخارجيين من تقديم أي خدمات تتعلق بالتدقيق للشركة التي شارك رئيسها التنفيذي CEO أو مديرها المالي CFO أو مدير حساباتها باعتباره أحد أعضاء مكتب التدقيق الخارجي على عملية التدقيق نفسها خلال السنة الأخيرة. وفي الحقيقة فإن هذا يعني أنه لا يمكن لشريك عملية التدقيق أن يتخلى عن العمل في التدقيق ليبدأ العمل مديراً تنفيذياً

في الشركة نفسها التي قام للتو بتدقيق حساباتها. في حين أن الموظفين والمديرين لا يزال بإمكانهم الانتقال من فريق مكتب المحاسبة القانونية لتولي مناصب مختلفة في الشركة الخاضعة لعملية التدقيق، فهذا الحظر يقتصر فقط على شركاء المحاسبة القانونية وقد كانت هناك بعض الأمثلة الواضحة على هذا التحول في الأدوار باعتبار ذلك جزءاً من مجمل الأحداث الخاصة بشركة إنرون.

الباب الثالث لقانون SOX: مسؤولية الشركة:

تحتوي اللوائح في الباب الثالث من قانون SOX على قواعد تنظيمية رئيسية تتعلق بلجان التدقيق وتصف معايير أداء لجان التدقيق ومجموعة كبيرة من قواعد حوكمة الشركات. فبموجب قانون SOX، يجب على جميع المؤسسات المسجلة أن يكون لديها لجنة تدقيق مكونة فقط من مديرين مستقلين. حيث يتبع مدققو مكتب التدقيق الخارجي لجنة التدقيق بشكل مباشر والمسئولة عن دفع أتعابهم والإشراف على أعمال التدقيق، وحل أي خلافات تقع بين التدقيق الخارجي والإدارة. وبالرغم من أن الشركات الأمريكية الكبرى قد كان لديها لجان تدقيق، فإن هذه القواعد قد تم استنتاجها من الممارسات التقليدية القديمة. على سبيل المثال، بينما كان لدى إدارات التدقيق الداخلي في السنوات الماضية علاقات ضعيفة خاصة بتقديم التقارير مع لجان التدقيق التابعين لها في كثير من الأحيان، فإن قانون SOX جعل هذه العلاقة أكثر قوة وأكثر فاعلية.

يجب أن يكون كل عضو من أعضاء لجنة التدقيق التابعة للمجلس (مجلس الإدارة) مديراً مستقلاً تماماً. ويجب أن يكون عضو واحد على الأقل من أعضاء لجنة التدقيق "خبيراً مالياً". وقد تم طرح هذه القوانين نتيجة جلسات الاستماع التي أدت إلى صدور قانون SOX، فقد تم اكتشاف أنه طلب من بعض أعضاء لجنة التدقيق المسؤولة عن شركة إنرون الذين كانوا على ما يبدو لا يعرفون الكثير عن المعاملات المالية القيام بعمليات المراجعة والاعتماد. وتُعرّف اللوائح التنظيمية لهيئة الأوراق المالية، والبورصة الأمريكية "الخبير المالي" على أنه الشخص الذي يملك، من خلال التعليم والخبرة، التالي:

- فهم وإدراك للمبادئ المحاسبية والقوائم المالية المتعارف عليها بشكل عام.

- خبرة في تطبيق هذه المبادئ المحاسبية المقبولة بشكل عام وربطها بمحاسبة التقديرات والمستحقات والاحتياطات التي يمكن مقارنتها عموماً بالتقديرات والمستحقات والاحتياطات في حال استخدم أي منها في القوائم المالية للشركة المسجلة.
- خبرة في إعداد أو تدقيق البيانات المالية التي تمثل القضايا المحاسبية الحالية التي يمكن مقارنتها عموماً بتلك القضايا المحاسبية المثارة في القوائم المالية لدى الشركة المسجلة.
- خبرة في الضوابط والإجراءات الداخلية الخاصة بالتقارير المالية.
- فهم وإدراك لمهام لجنة التدقيق.

ولا تتطلب هذه المبادئ أي شهادات رسمية أو خلفيات أكاديمية أو مؤهلات أخرى. فهي تنص على أنه يجب على أعضاء لجنة التدقيق أن يقدموا أنفسهم على أنهم على مستوى معين من المعرفة حول قضايا المحاسبة والتقارير المالية والضوابط الداخلية. ففي بعض الأحيان يُطلب من عضو لجنة التدقيق أن يضع نفسه أو تضع نفسها في خط المواجهة في حال كانت المؤسسة يتم استجوابها دائماً فيما يخص بعض القرارات الخاصة بالمسائل المالية والرقابة الداخلية.

ويدعو قانون SOx أيضاً لجان التدقيق إلى أن تقوم بوضع إجراءات لتلقي وحفظ ومعالجة الشكاوى المقدمة ومعالجة إفادات المبلغين المتعلقة بالقضايا المحاسبية ومسائل التدقيق المشكوك فيها. هذا في الحقيقة يعني أن لجنة التدقيق يجب أن تصبح، في الواقع، كياناً مستمراً شبه مستقل، بدلاً من أن تكون مجموعة فرعية من المجلس الإداري التقليدي الذي يلتقي في مكان ما ويجتمع كل ثلاثة أشهر. وبينما هذا الأمر يبدو فكرة جيدة، فإن معظم وظائف لجنة التدقيق لا تملك مصادر داعمة لخدمة إدارة المبلغين على المستوى المؤسسي، ويكون هذا الأمر غالباً من اختصاص إدارة أخلاقيات العمل على المستوى المؤسسي. وعلى الرغم من النصوص الموجودة في قانون SOx، فإنه يتم تشغيل الإدارات الخاصة بالمبلغين على مستوى لجنة التدقيق في الأساس بحسب الظروف.

كانت الشركات الأمريكية قبل صدور قانون SOx تقوم بحفظ قوائمها المالية داخل ملفات لدى هيئة الأوراق المالية والبورصة الأمريكية، ولكن لم يكن مديرو الشركات

المسؤولون الذين وقعوا على هذه التقارير المالية يتحملون أية مسؤوليات شخصية. الآن تم إزالة هذه العقبة. وأصبح واجباً أن يصدق الرئيس التنفيذي CEO أو المسؤول المالي الأساسي أو غيرهم ممن يمارسون مهام مشابهة على كل تقرير مالي سنوي أو ربع سنوي تم إرساله. لذلك يجب على المسئول الذي يقوم بالتوقيع، وكجزء مما أشير إليه بالبند ٣٠٢، أن يشهد:

- أن الموظف الذي يقوم بالتوقيع على التقرير قد قام بمراجعته.
- بناء على معرفة هذا الموظف الموقع، فإن القوائم المالية لا تحتوي على أي معلومات مادية مضللة أو غير صحيحة.
- مرة أخرى فإنه بناء على معرفة الموظف الذي يقوم بالتوقيع، فإن القوائم المالية تُمثل بعدالة الأوضاع والنتائج المالية لعمليات التشغيل في المؤسسة.
- أن المسئول الذي يقوم بالتوقيع مسؤول عن:
 - o وضع ضوابط داخلية والحفاظ عليها.
 - o أن تكون تلك الضوابط الداخلية قد صُممت لضمان أن المعلومات الجوهرية عن الشركة والشركات التابعة لها قد تم إعلامها للمسئول الموقع خلال الفترة التي تم فيها إعداد التقارير.
 - o أن تكون الضوابط الداخلية في المؤسسة قد تم تقييمها في غضون ٩٠ يوماً قبل إصدار التقرير.
 - o أن تشمل هذه التقارير المالية على تقييم الموظف الموقع لفاعلية تلك الضوابط الداخلية حتى تاريخ التقرير.
- يجب أن يفصح المسئول الموقع للمدققين الخارجيين ولجنة التدقيق ومديرين آخرين بأنه قد تم الكشف أو التصريح لمدققي حسابات الشركة عن أي نقص أو خلل مؤثر في تصميم وتشغيل الضوابط الداخلية التي قد تؤثر في دقة البيانات المالية المقدمة.
- ويجب أيضاً على المسئول الموقع أن يشير إلى ما إذا كان هناك ضوابط داخلية أو تغيرات أخرى قد أثرت بشكل جوهري في تلك الضوابط، وإلى الإجراءات التصحيحية التي جاءت بعد تاريخ تقييم الضوابط الداخلية.

من المعلوم أن قانون SOx يفرض عقوبات جنائية محتملة سواء بالغرامة المالية أم بالسجن على الأفراد المخالفين للقانون، كما أن المتطلبات الخاصة بحوكمة المؤسسة التي قامت بالتوقيع تضع عبئاً ثقیلاً على كاهل المسؤولين في الشركة. لذلك يجب على المسؤولين في الشركة أخذ كل التدابير اللازمة للتأكد من التزامهم بالقانون.

وقد أثار هذا المطلب الخاص بالتوقيع الشخصي مخاوف كبيرة لدى الرؤساء التنفيذيين CEOs والمديرين الماليين CFOs في الشركات كما تسبب في وجود قدر كبير من العمل الإضافي بالنسبة لموظفي قطاعي المحاسبة والمالية من أجل تحضير تلك التقارير وكذلك للمسؤولين الموقعين. تحتاج المؤسسة لوضع إجراءات تفصيلية لمعالجة البيانات الظاهرة في أسفل الوثيقة بحيث يكون المديرون الموقعون مطمئنين إلى استخدام عمليات فعالة وحسابات لإعداد تقارير جميعها موثقة بشكل جيد. قد ترغب المؤسسة في استخدام عملية مطولة للحصول على التوقيعات النهائية، التي يتم استخدامها لكي يقوم الموظفون الذين يُسلمون التقارير المالية بالتوقيع على ما يقومون بتسليمه. الشكل التوضيحي (٢-٣) يوضح مثال لأحد أنواع القرارات الخاصة بموافقة المسئول على الإفصاح والتي يطلب من المسؤولين التوقيع عليها. وبالرغم من أن هذا الإقرار الموضح في هذا الشكل ليس أحد النماذج الرسمية الخاصة بمجلس الإشراف المحاسبي على الشركات المساهمة، فإنه يستند إلى وثائق هيئة الأوراق المالية والبورصة الأمريكية، ويوضح أنواع الأمور التي سيطلب من المدير المسئول التصديق عليها. لقد قمنا بتسليط الضوء على عبارتين من العبارات الموجودة في الشكل التوضيحي (٢-٣) بوضعهما بخط عريض ومائل. وفقاً لقانون SOx فإن الرئيس التنفيذي CEO أو المدير المالي CFO مطالب بالتصديق الشخصي على هذه الأنواع من البيانات وقد يكون عرضة لمساءلة جنائية في حالة عدم صحة ما صدق عليه. وعلى الرغم من المخاطرة التي يتعرض لها المدير المسئول، فإنه يجب على فريق الدعم، متضمناً ذلك المدققين الداخليين، أخذ كل الاحتياطات اللازمة والممكنة للتأكد من صحة البيانات المقدمة للمسؤول الأعلى.

الباب الرابع لقانون SOx: تعزيز حالات الإفصاح عن البيانات المالية:

تم تخصيص هذا الباب من قانون SOx لتصحيح بعض المشاكل المتعلقة بالإفصاح عن التقارير المالية وللتشديد على قواعد تضارب المصالح بالنسبة للمسؤولين والمديرين،

وإلزام الإدارة بعمل تقييم للضوابط الداخلية، والمطالبة بعمل مدونة لقواعد السلوك خاصة بكبار المديرين وغيرها من الأمور، حيث يوجد هنا العديد من الأدوات. إن العديد من حالات الإفلاس غير المتوقعة والإخفاقات المفاجئة في جني الأرباح التي وقعت تقريباً في الوقت الذي انهارت فيه شركة إنرون نحو عام ٢٠٠٢ م قد نُسبت إلى تقارير مالية شديدة العدوانية، إن لم تكن محل شك. فقد لجأت الشركات وبلا حدود وبموافقة المدققين الخارجيين إلى اتباع بعض الأساليب غير اللائقة كالإعلان عن أرباح وهمية غير صحيحة في النتائج المدونة في التقارير، أو القيام بتحويل مقر قيادة الشركة إلى الخارج لتقليص حجم الضرائب. وعلى الرغم من أن هذه الأساليب كان يُسمح بها سابقاً وفقاً للمبادئ المحاسبية المقبولة قبولاً عاماً GAAP، والمعايير الدولية لإعداد التقارير المالية (International Financial Reporting Standards (IFRS) وبعض القوانين الموضوعية وقتها، فإن قانون SOx قد غير هنا العديد من القواعد وجعل من الصعب أو من غير القانوني استخدام مثل هذه الأساليب في الإفصاحات المالية.

إحدى الأساليب التي شاعت وقتها، هو ما كان يطلق عليه تقارير مالية صورية وقد استخدمت هذه الأساليب مراراً وتكراراً لتقديم صورة "وصفية" عن الوضع المالي للشركة من خلال إغفال نفقات الأرباح غير المتكررة مثل تكاليف إعادة الهيكلة أو التكاليف المتعلقة بالاندماج. من ناحية أخرى، فبسبب عدم وجود تعريف معياري موحد أو شكل ثابت للتبليغ عن الأرباح الشكلية، واعتماداً على الافتراضات المستخدمة، فقد كان من الممكن أن تصبح خسائر التشغيل أرباحاً في تقارير الأرباح الصورية. كانت المشكلة بالنسبة لهاتين المجموعتين من الأرقام أن المستثمرين والصحافة في معظم الأحيان يتجاهلون أرقام المبادئ المحاسبية المقبولة قبولاً عاماً GAAP، ويركزون أكثر على النتائج الشكلية التي يفضلونها. تتطلب القواعد الإلزامية لقانون SOx أنه يجب ألا تحتوي القوائم المالية المعلنة على أي بيانات مادية غير حقيقية أو أن تهمل أية حقيقة يمكن أن تجعل التقرير مضللاً. إضافة إلى ذلك، فإن النتائج الصورية أيضاً يجب أن تتوافق مع الظروف والنتائج المالية لعمليات التشغيل وفقاً للمبادئ المحاسبية المقبولة قبولاً عاماً GAAP.

شكل توضيحي (٣-٢)

إقرار المسئول بالإفصاح طبقاً لقانون SOx

إقرار الموظف بخصوص الامتثال لقانون SOx
<p>هذه شهادة إحاطة بأننا نعتزم الاعتماد على هذه البيانات، وإن الموقع أدناه يشهد، ويقدم ويتعهد لكل منها (هذه البيانات) وللشركة بالتالي:</p> <p>١. أنني قرأت تلك الأجزاء من المسودة المرفقة بالمغلف والتي تتصل بشكل مباشر بنطاق مسئوليتي كموظف بالشركة ("المعلومات المعتمدة").</p> <p>٢. استناداً إلى معرفتي فإن المعلومات المعتمدة وحتى نهاية الفترة التي يغطيها هذا المغلف لا تحتوي على بيان مالي غير صحيح لأي واقعة مادية ولم تهمل الإفصاح عن واقعة مادية ضرورية تجعل البيانات - في ظل الظروف التي أعدت فيها البيانات - غير مضللة.</p> <p>٣. استناداً إلى معرفتي فإنه في حدود نطاق المعلومات المعتمدة، فإن المعلومات المعتمدة قد تم تقديمها بصورة نزيهة، في جميع النواحي الجوهرية، والوضع المالي، ونتائج العمليات، والسيولة النقدية للشركة كما في نهاية الفترة المعروضة في المغلف أو على مقربة منها.</p> <p>٤. لستُ على علم بأي قصور في فاعلية ضوابط وإجراءات الإفصاح الخاصة بالمؤسسة والتي قد تؤثر بصورة سلبية في قدرة الشركة في تسجيل، ومعالجة، وتلخيص، وإعداد تقرير عن المعلومات المطلوب الإفصاح عنها في المغلف.</p> <p>٥. لستُ على علم بأي قصور ملموس أو نقطة ضعف جوهرية في تصميم وتشغيل الضوابط الداخلية في الشركة والتي قد تؤثر بصورة سلبية على قدرة الشركة في تسجيل، ومعالجة، وتلخيص وإعداد تقارير البيانات المالية.</p> <p>٦. لستُ على علم بأي احتيال، سواء كان مادياً أم غير مادي، فيما يخص إدارة الشركة أو موظفين آخرين من الذين يلعبون أدواراً أساسية في الضوابط الداخلية للشركة.</p> <p>التوقيع: _____</p> <p>التاريخ: _____ يوم _____ ٢٠xx</p> <p>الاسم: _____</p> <p>المسمى الوظيفي: _____</p>

ربما كانت القضية الأبرز التي أسهمت في إسقاط شركة إنرون هي وجود عدد كبير من المعاملات الخارجة عن الميزانية العامة التي لو تم دمجها بالتقارير المالية المعتادة، لاتضحت المشاكل المالية الرئيسية. وبمجرد اكتشافها وتضمينها مع النتائج المالية الأخرى لشركة إنرون والإفصاح عنها، قد دفع ذلك شركة إنرون نحو الإفلاس. أما الآن فيشترط قانون SOx إعداد تقارير ربع سنوية وسنوية للإفصاح فيها عن مثل هذه العمليات التي تتم خارج الموازنة والتي قد يكون لها تأثير جوهري في التقارير المالية الحالية أو المستقبلية. قد تتضمن هذه العمليات التزامات طارئة Contingent obligations، أو علاقات مالية مع كيانات غير موحدة، أو أمور أخرى قد يكون لها تأثيرات مادية على عمليات التشغيل. تشترط القواعد النهائية هنا — بعد تمرير قانون SOx — أن تقوم كل مؤسسة بتقديم توضيح عن إجراءاتها المتعلقة بالخروج عن الميزانية "مناقشة وتحليل الإدارة" (Management's Discussion and Analysis (MD&A في النموذج السنوي 10K.

أحكام وإفصاحات وقواعد أخلاقية موسعة لمعالجة تضارب المصالح:

صورت جلسات الاستماع التي أدت إلى إقرار قانون SOx في كثير من الأحيان مسئولي ومديري الشركات بأنهم جشعون وطماعون بشكل كبير. فبعض الإجراءات كانت تبدو متضاربة في المصالح، بدلات الانتقال الضخمة أو القروض الشخصية التي مُنحت للمديرين التنفيذيين في الشركات وتم إعفاؤهم من سدادها بعد ذلك بأمر من مجالس إدارة الشركات، فالرئيس التنفيذي CEO، على سبيل المثال، عندما يطلب من مجلس إدارة الشركة أن يتم منح قرض شخصي لمديره المالي CFO بشروط سداد غامضة مع أحقية المطالبة بسداده أو الإعفاء منه، فإن هذا بالتأكيد يخلق حالة من تضارب المصالح. وعلى الرغم من أن هناك مجموعة من الاستثناءات المسموح بها، فإن قانون SOx اعتبر أنه من غير القانوني بالنسبة لأي شركة أن تقوم، سواء بشكل مباشر أو غير مباشر بتمديد الائتمان - المعطى في صورة قرض شخصي - لأي مسئول أو مدير.

ولكونه أحد العناصر الهامة في الحوكمة المؤسسية، يطالب قانون SOx جميع المؤسسات باعتماد مدونة خاصة بقواعد السلوك المهني وأخلاقيات المهنة لكبار المديرين الماليين لديها

وأن تفصح عن الالتزام بهذه المدونة باعتبارها جزءاً من تقاريرهم المالية السنوية. وفي الوقت الذي جعل فيه قانون SOx هذا الأمر أحد المتطلبات الخاصة بكبار المسؤولين، فقد كانت هناك مدونات معتمدة لقواعد السلوك الوظيفي والأخلاقي في بعض المؤسسات لسنوات عديدة. وقد قامت تلك المؤسسات بتطويرها إلى إدارات أكثر رسمية لأخلاقيات المهنة في الشركات الكبرى، وكان ذلك في مطلع التسعينيات من القرن الماضي، إلا أنها كانت توضع غالباً من أجل الموظفين والمشرفين بدلاً من وضعها لمسئولي الشركات. وقد تم في هذه المدونات تعريف مجموعة من القواعد أو السياسات التي تم تصميمها لتطبق على جميع الموظفين، والتي شملت العديد من المسائل مثل السياسات المفروضة على حماية سجلات الشركة أو السياسات المفروضة على قبول الهدايا وغيرها من القضايا والفوائد الأخرى.

في ظل نمو الاهتمام العام حول الحاجة إلى ممارسات قوية للحوكمة وأخلاقيات العمل، فقد قامت العديد من المؤسسات بتعيين موظف مسؤول عن أخلاقيات المهنة لإطلاق مثل تلك المبادرة، من خلال مدونة لقواعد السلوك في خطوة أولى. ولم يتناول قانون SOx محتوى مدونة أخلاقيات المهنة هذه على مستوى المؤسسة، ولكن ركز على الحاجة إلى المعايير نفسها بالنسبة لكبار المسؤولين كما هي لجميع الموظفين الآخرين في الشركة. كما يطالب قانون SOx على وجه التحديد أنه يجب على مدونة قواعد السلوك المهني أو مدونة أخلاقيات المهنة الخاصة بكبار مسؤولي المؤسسة أن تعزز وبصورة معقولة:

- السلوك النزيه والأخلاقي، متضمناً ذلك التعامل الأخلاقي مع التضارب الفعلي أو الظاهري في المصالح بين العلاقات الشخصية والعلاقات المهنية.

- إفصاح شامل ودقيق وعادل في الوقت المناسب ومفهوم في التقارير المالية للمؤسسة.

- الامتثال للقوانين واللوائح الحكومية المعمول بها.

إذا كانت المؤسسة تمتلك مدونة خاصة بالقواعد السلوكية، فيتعين على الإدارة التأكد من أن هذه المدونة يتم تطبيقها على جميع أعضاء المؤسسة، وأنها متوافقة مع قانون SOx، وأن هذه القواعد الأخلاقية قد تم الإفصاح عنها إلى جميع أعضاء المؤسسة، متضمناً ذلك المسؤولين. إن القضية الجوهرية للحوكمة هنا هي التأكد من أن المدونة الحالية لقواعد السلوك تغطي قواعد قانون SOx السابقة، وأنه قد تم إيصالها إلى الإدارة العليا، وأن هؤلاء

المسؤولين قد وافقوا على الالتزام بها. وعلى الرغم من أن عمليات وإجراءات الامتثال بقانون SOx قد وُضعت فقط لكبار المديرين في المؤسسة، فإنه هذا هو الوقت المثالي لإطلاق إدارة أخلاقيات المهنة في جميع أنحاء المؤسسة والتي يمكن تطبيقها على الإدارة العليا وكذلك جميع الموظفين.

ليس الأمر مطلباً شرعياً لقانون SOx فحسب، إذ إن مجموعة فعالة من المعايير الأخلاقية يمكن أن تعبر بالمؤسسة من وضع كارثي وتساعد على التحول في الاتجاه الصحيح. كان الدافع وراء سن قانون SOx وأحكامه القوية في هذه المجالات هو إدراك أن بعض مسؤولي الشركات كانوا يعملون بهدف تحقيق مصالح ومكاسب شخصية دون أي اعتبار للقيم الأخلاقية الراسخة كما ثبت من خلال التقارير المالية الدقيقة والسليمة. وتستطيع المتطلبات الأخلاقية للمهنة في قانون SOx أن تساعد أي مؤسسة على أن تضع لنفسها قدماً من أجل تحسين الممارسات المتعلقة بالحوكمة وسلوكيات الأعمال الأخلاقية بشكل أفضل.

قواعد ومتطلبات أخرى لقانون SOx:

يتضمن قانون SOx مجموعة كبيرة ومعقدة من القواعد والأحكام التي تغطي مجالات عديدة كالمتطلبات الخاصة بحوكمة لجنة التدقيق، وتضارب مصالح المحلل الأمني وغيرها من قواعد الإفصاح المالي. لسنا هنا بصدد تقديم شرح تفصيلي عن كامل القانون وأحكامه. فمن منظور الحوكمة المؤسسية وحوكمة تقنية المعلومات، فإن فهم وإدراك البند ٤٠٤ وبعض القضايا الأخرى التي تم تسليط الضوء عليها في هذا الفصل ربما يكون هو الأكثر أهمية. ويمكن إيجاد الوصف العام الأكثر تفصيلاً لقانون SOx في الكتاب الذي أشار إليه المؤلف سابقاً حول قانون SOx.

يعد قانون SOx منذ إقراره قانوناً أمريكياً في مطلع التسعينيات من القرن الماضي أحد العناصر الهامة في التشريع، فقد أسهم منذ ذلك الوقت في تغيير العديد من القضايا المتعلقة بالتقارير المالية، والممارسات الخاصة بالرقابة الداخلية، والحوكمة المؤسسية. وعلى الرغم من بعض التغيرات التي طرأت على بعض عناصر قانون SOx منذ صدوره وأن متطلباته لا تثير الكثير من الاهتمام، فإن معظم جوانب قانون SOx لا تزال فعالة وقابلة للتطبيق. لقد كان الجزء الأكبر في التغيير هو إطلاق معيار التدقيق رقم 5 AS، وقد تمت مناقشته من قبل، وهو أحد معايير التدقيق التي تصف نهجاً أكثر اعتماداً على المخاطر لمراجعة

وتقييم الضوابط الداخلية. وقد احتوى قانون SOx في الأصل على بعض القواعد الخاصة بالتبليغ عن المخالفات التي سمحت لجميع الموظفين بكتابة تقارير بصورة مستقلة للتبليغ عن أي احتيال مالي محتمل. وكانت تُصرف مكافآت وحوافز مادية لأصحاب تلك التقارير الشخصية الخاصة بالتبليغ. وعلى الرغم من أنه كان من المفترض أن يتسبب ذلك في عاصفة من الدعاوي القضائية، فإنه لم يكن هناك الكثير منها لأي نشاط من الأنشطة الخاصة بقانون SOx في هذا الجانب منذ إقراره وتمريه.

وعلى الرغم من أنه سيتم تناول العديد من التفاصيل الخاصة بهذا القانون من قبل كل من الإدارة المالية والمدققين الداخليين والخارجيين، فإنه يجب أن يكون لدى المسئول التنفيذي للأعمال اليوم إدراك عام جيد لقواعد ومتطلبات قانون SOx. كما يجب أن يساعد الوصف العام لهذا القانون الذي جاء في ثنايا هذا الفصل مسئولي الأعمال التنفيذيين اليوم على فهم قانون SOx وأهميته في حوكمة تقنية المعلومات على نحو أفضل.

ما المقصود بحوكمة تقنية المعلومات:

كما هو موضح في مقدمة هذا الفصل، فإن نظام حوكمة تقنية المعلومات IT Governance عبارة عن مجموعة فرعية من القضايا الشاملة لحوكمة المؤسسات وأحد العناصر الهامة للغاية في هذا المجال. لا يوجد تعريف واحد معتمد لحوكمة تقنية المعلومات، ويوضح البحث من خلال شبكة الإنترنت أن حوكمة تقنية المعلومات تعني أشياء مختلفة لأشخاص مختلفين:

- تُستخدم حوكمة تقنية المعلومات في كثير من الأحيان لوصف العمليات الضرورية لاتخاذ قرار بشأن الأموال التي يجب إنفاقها على موارد تقنية المعلومات. تتضمن عملية حوكمة تقنية المعلومات هذه وضع أولويات للاستثمارات في تقنية المعلومات وتبريرها. كما تتضمن الضوابط المفروضة على الإنفاق مثل الموازنات ومستويات الصلاحية.

- تستخدم حوكمة تقنية المعلومات في كثير من الأحيان لوصف العديد من الجوانب المختلفة في التغيرات التي تطرأ على تقنية المعلومات. فعلى المستوى الأدنى، قد تستخدم في بعض الأحيان لوصف إدارة المشاريع والتحكم في محفظة المشاريع المتعلقة بتقنية المعلومات. كما هو موضح في الفصل السادس عشر من هذا الكتاب.

- تستخدم حوكمة تقنية المعلومات لضمان امتثال عمليات التغيير في تقنية المعلومات للمتطلبات التنظيمية سواء كانت قوانين ولوائح حكومية أم معايير مهنية.
 - حوكمة تقنية المعلومات هي عملية المواءمة بين التغيير المطلوب في تقنية المعلومات والإنفاق عليها وبين متطلبات الأعمال ونفقاتها. وقد تشمل حوكمة تقنية المعلومات في بعض الأحيان أيضاً آلية توزيع وانتشار فريق تقنية المعلومات.
 - تُستخدم حوكمة تقنية المعلومات أيضاً لوصف إدارة وضبط خدمات تقنية المعلومات. على سبيل المثال، تستخدم اتفاقيات مستوى الخدمة (service level agreements SLAs) (التي سنتحدث عنها في الفصل السابع عشر من هذا الكتاب) لتحديد مستويات الخدمة المقبولة للأعمال، ثم استخدمت بعد ذلك أساساً لمتابعة الخدمات.
 - تضمن حوكمة تقنية المعلومات حل المشاكل اليومية وكذلك دعم جميع موارد تقنية المعلومات لتتماشي مع متطلبات العمل.
- تتعامل حوكمة تقنية المعلومات بشكل أساسي مع العلاقة بين تركيز أعمال المؤسسة (ما تركز عليه أعمال المؤسسة) وإدارة وتشغيل تقنية المعلومات في المؤسسة. يُبرز مفهوم حوكمة تقنية المعلومات أهمية الأمور المتعلقة بتقنية المعلومات، كما يؤكد ضرورة أن تكون القرارات الإستراتيجية لتقنية المعلومات بيد أعلى مستويات الإدارة في الشركة متضمناً مجلس الإدارة بدلاً من أن تكون بيد إدارة تقنية المعلومات فقط مثل الرئيس التنفيذي للمعلومات CIO. في الواقع، لقد تطورت مفاهيم حوكمة تقنية المعلومات منذ الأيام الأولى لظهور تقنية المعلومات عندما تخلت الإدارة العليا في كثير من الأحيان عن سلطة عمليات تشغيل تقنية المعلومات وتمويلها لصالح أخصائيين يُطلق عليهم الرؤساء التنفيذيون للمعلومات CIOs، ولكنهم لم يديروا موارد تقنية المعلومات بقوة من منظور الإدارة الشاملة.

وقد كانت نتائج تلك العملية في الواقع متمثلة في ظهور بعض العمليات الممتازة لتقنية المعلومات التي أحدثت تحولاً كبيراً في العديد من الشركات الرائدة في جميع أنحاء العالم وحسنت من كفاءاتها وزادت من أرباحها، ومع كل ذلك، فقد عانت العديد من المؤسسات الأخرى من بعض الإخفاقات الجسيمة (الانهيار الكلي) في تقنية المعلومات،

وكان ذلك بسبب التخطيط السيئ للمشروعات، تجاوز التكاليف، وإخفاقات على مستوى فهم القائمين على الأعمال وتقنية المعلومات لقضايا تقنية المعلومات، وغيرها من الأمور. على سبيل المثال، كشف استطلاع رأي أجرته مؤسسة غارتنر في عام ٢٠٠٢ أن ٢٠٪ من مجموع الأموال التي تم إنفاقها على تقنية المعلومات قد أهدرت، وهذه النتيجة تمثل، على الصعيد العالمي، تدميراً لما قيمته الإجمالية قرابة ٦٠٠ مليار دولار أمريكي سنوياً. وقد كشف الاستطلاع الذي أجرته شركة آي بي إم (IBM) سنة ٢٠٠٤ لأكثر من ١٠٠٠ من الرؤساء التنفيذيين للمعلومات CIOs بأنهم يعتقدون أن، في المتوسط، قرابة ٤٠٪ من مجمل الإنفاق على تقنية المعلومات لم يحقق أي عوائد لمؤسساتهم^(٤). وفي السنوات الأخيرة، كشفت استطلاعات رأي أخرى أن ما بين ٢٠٪ إلى ٧٠٪ من الاستثمارات الضخمة في مشاريع تقنية المعلومات يتم إهدارها بصفة مستمرة، مما يعد عائقاً أو إخفاقاً في تحقيق أي عوائد أو فوائد لمؤسساتهم. كل ذلك يشير إلى الحاجة إلى نظم قوية لحوكمة تقنية المعلومات المؤسسية. فبدلاً من الجدل القائم حول تحديد التعريف الأفضل والأصلح لحوكمة تقنية المعلومات، فإنه يجب على كبار مديري المؤسسات النظر إلى عناصر التشابه بين جميع التعريفات الواردة. ففي كل حالة تقريباً تشتمل الحوكمة على مزيج مما يلي:

- التحكم في جميع الجوانب الخاصة بعمل تقنية المعلومات.
- التنسيق بين الأجزاء المختلفة للأعمال المرتبطة بتقنية المعلومات — مثل تطوير النظم الجديدة للبنية التحتية لتقنية المعلومات.
- قياس مخرجات نظم وعمليات تقنية المعلومات.
- الامتثال للسياسات الداخلية لتقنية المعلومات.
- تبرير الإنفاق على جميع موارد تقنية المعلومات.
- المساءلة والشفافية على مستوى إدارة تقنية المعلومات والمؤسسة.
- روابط قوية مع الاحتياجات الخاصة بعملاء تقنية المعلومات، وواسعة النطاق للمؤسسة، وغيرهم من أصحاب المصلحة.

إن العديد من قضايا حوكمة تقنية المعلومات تلك معنية بسمات نظم تقنية المعلومات نفسها متضمنة قضايا التقنية الحديثة، والنظم القديمة التي تستخدم تقنيات قديمة، الأمن والتوثيق، والعديد من القضايا الأخرى. إن معالجة مثل تلك المسائل الخاصة بحوكمة تقنية المعلومات ليست بالأساس مسألة تقنية، وإنما هي مسألة إدارية.

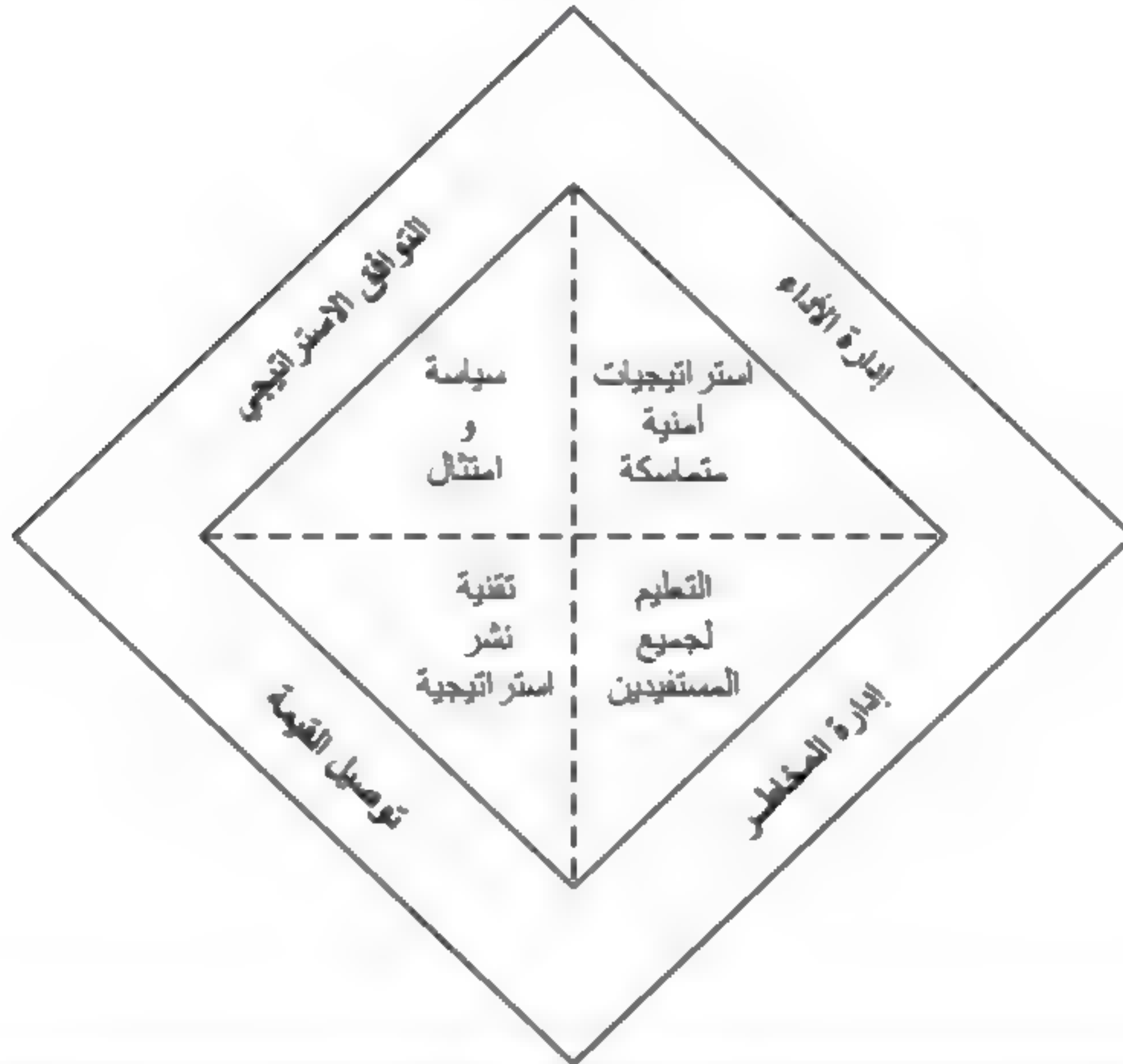
لعل السمة الأبرز في القضايا الخاصة بحوكمة تقنية المعلومات في هذا الفصل وغيره من الفصول اللاحقة هي أن موارد وقدرات تقنية المعلومات في المؤسسة لم تعد شيئاً غير مفهوم من جانب الأعمال في المؤسسة، على الجانب الآخر يتعين أيضاً على تقنية المعلومات هذه أن تفهم الأعمال واحتياجاتها. يجب أن تكون القضايا الجوهرية لتقنية المعلومات إحدى المسائل التي تخص المديرين التنفيذيين على مستوى مجلس الإدارة، إلا أنه بسبب الطبيعة التقنية لتقنية المعلومات قد تُترك بعض القرارات الرئيسية لأخصائيي تقنية المعلومات. إن حوكمة تقنية المعلومات عبارة عن النظام الذي يملك فيه جميع أصحاب المصالح، ومن ضمنهم مجلس الإدارة والعملاء المحليون وغيرهم كالمالية، المدخلات الضرورية لعملية صنع القرار.

ستناقش الفصول التالية العديد من الجوانب والافتراضات المتعلقة بحوكمة تقنية المعلومات. وستركز بشكل عام على قضايا المخاطر المؤسسية، وقضايا حوكمة تقنية المعلومات، ومسائل قانونية ونظامية وقضايا أمن المعلومات، والتهديدات الداخلية والخارجية التي تؤثر في حوكمة تقنية المعلومات.

تتوافق جميع أهداف حوكمة تقنية المعلومات داخل نموذج شامل، كما هو موضح بالشكل التوضيحي (٤-٢). تكون حوكمة تقنية المعلومات محاطة بمفاهيم إدارة الأداء، والتوافق الإستراتيجي، وإدارة المخاطر، وتوصيل القيمة. ولتحقيق ذلك، هناك حاجة إلى سياسة قوية، وممارسات امتثال، وعمليات لإدارة الأداء والمخاطر، وفهم شامل للتوصيل المناسب للقيمة. يعرض الشكل التوضيحي (٤-٢) هذه المفاهيم على مستوى رفيع، غير أنه سيتم الرجوع إليها بالتفصيل في فصول لاحقة.

شكل توضيحي (٢-٤)

أهداف حوكمة تقنية المعلومات



قضايا المخاطر المؤسسية لحوكمة تقنية المعلومات:

تواجه كل مؤسسة مجموعة كبيرة من المخاطر، تشمل عمليات تشغيل الأعمال المؤسسية، والعوامل الخاصة بسوق العمل وما يتصل بها، والأوضاع الاقتصادية العامة، وقائمة غير منتهية من العوامل الأخرى من المخاطر المؤسسية. وعلى الرغم من أن هذا الكتاب لا يسعى لتقديم ومناقشة جميع الجوانب الرئيسية المتعلقة بإدارة المخاطر على مستوى المؤسسة وما يعرف بإطار عمل إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية^(٥) (COSO) enterprise risk management (COSO ERM)؛ فإن هناك العديد من الجوانب المتعلقة بالإدارة الشاملة للمخاطر المؤسسية، وهي جوانب هامة بالنسبة

للممارسات الفعالة لتقنية المعلومات على وجه التحديد. سيقدم الفصل الرابع من هذا الكتاب معلومات أكثر حول لجنة المنظمات الراعية COSO.

ولكي تمتلك المؤسسة ممارسات فعالة لحوكمة تقنية المعلومات، فهي بحاجة إلى أن يكون لديها برنامج فعال لتقييم وإدارة المخاطر الشاملة، والمخاطر المؤثرة داخل المؤسسة، والمخاطر النوعية التي تواجه عمليات التشغيل الخاصة بتقنية المعلومات. يعرض الشكل التوضيحي (٢-٥) بإيجاز بعض القضايا الخاصة بمخاطر حوكمة تقنية المعلومات ويلخص بعض الإستراتيجيات الفعالة في إدارة تلك المخاطر.

ما يواجه كبار المديرين غالباً اعتراضات شديدة أو بسيطة عندما يقومون بقبول وإدارة العديد من أنواع المخاطر المتعلقة بتقنية المعلومات. خير مثال على ذلك كلمة السر المستخدمة في النظم للوصول لموارد تقنية المعلومات. فتبعاً لأحد الاتجاهات، قد يحتاج المدير غير الملم بالتقنية بشكل جيد إلى أن يستخدم أسلوباً بسيطاً وسهلاً التذكر لكلمة المرور، والتي تكون غالباً مكونة من ثلاثة حروف تمثل الأحرف الأولى من اسمه الثلاثي ورقم. فالسيدة Mary Anne Jones قد تستخدم MAJ1 كلمة مرور للوصول إلى النظم الخاصة بها، ويمكن تغيير كلمة المرور فقط من خلال تغيير الرقم المكون من عدد واحد من آن لآخر عند تغيير كلمات المرور. وبذلك يكون هذا النظام سهل التذكر ولكن يمكن اختراقه بسهولة.

يؤيد أخصائيو أمن المعلومات عادة الذهاب إلى الاتجاه الآخر وهو وضع معايير لكلمة المرور، تكون غالباً مركبة من ثمانية حروف أو أكثر منها حروف كبيرة وصغيرة، بالإضافة إلى الأرقام والرموز الخاصة وجميعها تتطلب تغييراً بصفة دورية. قد يخلق ذلك جواً أكثر أماناً وسرية، إلا أن الكثيرين قد تكون لديهم مشكلة في استدعاء كلمات المرور هذه والتي يصعب تذكرها، ومن ثم يقومون بكتابتها على أوراق ملاحظات لاصقة ووضعتها على لوحات المفاتيح الخاصة بحواسيبهم.

شكل توضيحي (٢-٥)

قضايا مخاطر حوكمة تقنية المعلومات

متطلبات المخاطر المؤسسية	استراتيجيات تفعيل المخاطر
فهم رغبة المؤسسة في المخاطر	عندما تُواجه المؤسسة بمخاطر اختيارية. فعليها أن تدرك مدى حجم ومستوى المخاطر التي ستحملها. فعندما تكون الإدارة مستعدة لقبول مشاريع أكثر مخاطرة، ينظر إليها بأن لديها شهية كبيرة للمخاطر.
فهم قبول المخاطر	ستواجه المؤسسة مخاطر عديدة. ولكن يجب أن يكون هناك فهم كافٍ وواضح لتحديد أي وحدة داخل المؤسسة هي التي ستقبل المخاطرة أو تتحمل مسئوليتها.
ضمان مشاركة الأشخاص المناسبين	يجب إسناد مسؤوليات الوحدة التنظيمية عن جميع المخاطر المحددة. كما يجب على الوحدة التنظيمية الإقرار بمسؤوليتها عن اتخاذ الإجراءات المناسبة في حال وقوع المخاطر.
قبول المخاطر المتبقية	من وجهة نظر المحاسبة أو التدقيق، تعتبر المخاطر المتبقية هي احتمالية أن المدقق لن يستطع الوصول إلى الخطأ الجوهرى الموجود في التقرير المالى للعميل ومن ثم سيقدم بشكل خاطئ تقريراً لا يحمل أي تحفظات حول دقة الحسابات. وبالمفهوم نفسه، قد تكون الإدارة غير مدركة للآثار المترتبة على المخاطر ومن ثم تقبل المخاطر أو تقر بهذه الأشياء.
فهم عمليات اختيار الرقابة	تحتاج المؤسسة إلى معرفة تكاليف ومقتضيات الضوابط المختلفة التي يمكن أن تقوم بوضعها استجابة لمختلف المخاطر المحددة.
معرفة تكاليف معالجة أحداث المخاطر	ستواجه المؤسسة العديد من المخاطر، لذا يجب أن يكون لديها معرفة جيدة بالتكاليف اللازمة لمعالجة مختلف الأمور في حال وقوع المخاطر المحددة.

وضع إستراتيجية واضحة للتخفيف من المخاطر	يجب أن يكون لدى المؤسسة إستراتيجية محددة ومسببة على نحو جيد حول ماهية الإجراءات أو التدابير التي يجب اتباعها في حال حدوث مخاطر مرتبطة بتقنية المعلومات.
فهم عمليات اختيار الرقابة	هناك العديد من الاعتبارات في حال حدوث مخاطر مرتبطة بتقنية المعلومات. لذا يجب على المؤسسة أن تقوم بتطوير الضوابط الملائمة التي سوف تقوم بمعالجة تلك المخاطر بطريقة فعالة.

إن الفكرة الرئيسية وراء متطلبات وإستراتيجيات المخاطر الموضحة في الشكل التوضيحي (٥-٢) هو أن المؤسسة بحاجة إلى أن يكون لديها معرفة بمختلف أنواع المخاطر المتعلقة بتقنية المعلومات التي تواجهها وكذلك التكاليف والإستراتيجيات البديلة لاتخاذ الإجراءات التصحيحية المتبعة في حال وقوع مثل تلك المخاطر. إن المصطلح أو المفهوم الهام جداً هنا هو ما يسمى الرغبة في المخاطر Risk Appetite. بمعنى، ما حجم المخاطر التي على استعداد أن يتقبلها أحد كبار المديرين أو المؤسسة بأكملها؟ فالمستثمر الفردي الذي يضع أمواله في سندات شركة تصنيفها (AA) يمتلك شهية مخاطر أقل بكثير من المستثمر الذي يضع أمواله في سوق أسهم شركات التقنية المضاربة.

إن الإلمام بقضايا المخاطر المؤسسية يعد مطلباً لتطبيق العمليات الفعالة لحوكمة تقنية المعلومات. إننا في الواقع نحتاج دائماً إلى أن ندرك أن كل مجال من مجالات تقنية المعلومات وعمليات التشغيل الشاملة للأعمال تشتمل على مخاطر لأنشطة أو أحداث غير مخطط لها. لذلك يجب أن يكون لدينا دائماً إستراتيجيات وعمليات معمول بها للاستجابة بشكل ملائم لتلك المخاطر في حال حدوث أي منها.

قضايا التنظيم المؤسسي لحوكمة تقنية المعلومات:

لقد توسعت قضايا واهتمامات حوكمة تقنية المعلومات لتصل إلى ما هو أبعد من إدارة تقنية المعلومات ومواردها فقط، بل يجب أن تشمل العديد من القضايا والاهتمامات على مستوى المؤسسة بأكملها. لذلك يجب علينا أن ننظر دائماً إلى مورد تقنية المعلومات في

المؤسسة بأنه ليس مجرد عنصر متفرد بل هو أحد الوحدات أو المكونات التي لها طبيعة خاصة بالنسبة للمؤسسة بأكملها. بعض تلك القضايا الخاصة بالحوكمة موضحة بالشكل التوضيحي (٦-٢).

إن الرسالة التي يريد الشكل التوضيحي (٦-٢) أن يبعث بها هي أنه على الرغم من أن إدارة تقنية المعلومات قد تقوم بتطوير عمليات وإجراءات للحوكمة تؤثر في نظم وعمليات تشغيل تقنية المعلومات الخاصة بها فإنه يجب عليهم التفكير دائماً في تلك العمليات والإجراءات في إطار أكبر من ذلك بكثير يشمل المؤسسة بأكملها. فعلى سبيل المثال، من السهل جداً نسيان أن هناك العديد من الإجراءات الخاصة بالحوكمة تؤثر في المسؤولية الائتمانية للمؤسسة وفي مديريها الأساسيين بوجه خاص للحفاظ على استثمارات المستثمرين وتعزيزها على جميع المستويات. إذ يمكن أن يؤدي الإخفاق أو القصور في هذا الأمر إلى رفع الدعاوى المدنية أو حتى القانونية على مديري المؤسسة. والاعتبار الذي له صلة هنا هو أن المؤسسة وعملياتها التشغيلية الخاصة بتقنية المعلومات لا يملكون مجموعة مفتوحة أو غير منتهية من الموارد لأخذ الإجراءات التصحيحية المناسبة. لذا يجب أن نوازن دائماً بين أثر اتخاذ الإجراءات التصحيحية وبين موارد المؤسسة بأكملها.

يشير الشكل التوضيحي (٦-٢) إلى قضايا الاختصاص والحدود على أنها أحد مكونات حوكمة تقنية المعلومات. فمع أنه قبل سنوات ليست بالكثيرة كانت موارد تقنية المعلومات في المؤسسة توضع خلف أبواب مغلقة محكمة السرية وتكون غالباً مرفقة في موقع منعزل عن باقي العمليات التشغيلية للمؤسسة، إلا أن هذا لا يجب أن يمنعنا في أن ننظر دائماً إلى العمليات التشغيلية الخاصة بتقنية المعلومات على أنها العنصر الرئيسي في عملية استمرار باقي العمليات التشغيلية الأخرى في المؤسسة. على أية حال، يجب علينا أن نتذكر دائماً أن هناك حدوداً موجودة، ويجب أن تدرك العمليات التشغيلية التقنية والمالية وغيرها الحدود بين مختلف مجالات المسؤولية عند وضع عمليات الحوكمة.

حوكمة تقنية المعلومات والقضايا التشريعية والتنظيمية:

بدأنا هذا الفصل بتقديم نبذة مختصرة عن بعض العناصر الأساسية في قانون SOx، وهو أحد العناصر الهامة في التشريع التي تؤثر في المراجعة والتقارير المالية وضوابطها الداخلية. وبالرغم من احتوائه على العديد من القواعد التشريعية الرئيسية، فإن SOx هو مجرد قانون من بين العديد من القوانين التنظيمية والتشريعية الرئيسية وحتى القوانين الثانوية التي تؤثر في العمليات التشغيلية لحوكمة تقنية المعلومات. يغطي بعض هذه القوانين كامل العمليات التشغيلية المؤسسية على المستوى المحلي أو الدولي. في حين يختص البعض الآخر بشكل أكبر بأمن تقنية المعلومات. وفي حالات أخرى، نجد أن العمليات التشغيلية لحوكمة تقنية المعلومات لا تتأثر بالقواعد والقوانين التشريعية الحكومية، ولكنها تتأثر بالمعايير المهنية غير الإلزامية ولكنها ضرورية للبقاء على الأقل في المنافسة.

ستقدم الفصول اللاحقة وتناقش بعض القضايا التشريعية والتنظيمية المتعلقة بحوكمة تقنية المعلومات بمزيد من التفصيل. على سبيل المثال، يقدم الفصل العاشر من هذا الكتاب نبذة عامة عن بعض من بين العديد من قوانين أمن تقنية المعلومات التي تؤثر في المؤسسة هذه الأيام. ويناقش الفصل الحادي عشر العناصر الهامة الخاصة بمعيار أمن البيانات الخاص بصناعة بطاقات الدفع (Payment Card Industry Data Security Standard (PCI DSS)، التي تعتبر مجموعة هامة من القواعد المؤثرة في أي مؤسسة تستخدم بطاقات الائتمان في العمليات التشغيلية الخاصة بأعمالها. وعلى المستوى الآخر، يقدم الفصل السابع من هذا الكتاب بعض المعايير العالمية في حوكمة تقنية المعلومات مثل معيار أيزو ٣٨٥٠٠ (ISO 38500)، والتي لا تعتبر قواعد تشريعية بل معايير امتثال يجب اتباعها من قبل أي مؤسسة ذكية.

شكل توضيحي (٦-٢)

قضايا حوكمة تقنية المعلومات المؤسسية

القضية على مستوى المؤسسة	الاعتبارات الخاصة بحوكمة تقنية المعلومات
عمليات رصد المخاطر في الشركات	هي أكثر من مجرد تحديد لأنواع ومستويات مختلفة للمخاطر المؤسسية والتقنية التي يمكن أن تؤثر في المؤسسة، لذا يجب أن تكون هناك عمليات معمول بها ومستمرة لتحديد حالة تلك المخاطر المحددة إلى جانب وجود خطط عمل سارية وذلك لاتخاذ الإجراءات المناسبة في حال وقوع المخاطر.
الآليات الضعيفة لاتخاذ القرارات	هي أكثر من مجرد مراقبة لحالة المخاطر المتعلقة بحوكمة تقنية المعلومات، لذا يجب أن تكون هناك عمليات إدارية معمول بها لاتخاذ الإجراءات المناسبة في حال وقوع المخاطر. ويعتبر ذلك صعباً خاصة في حال اشتمل الإجراء المخطط له على بعض الأمور كإيقاف تشغيل الشبكة التقنية، وهو الأمر الذي يتطلب قرارات إدارية قوية وحاسمة.
مخاطر انتهاك خصوصية سجلات البيانات الخاصة وبيانات الأعمال	سواء كانت سجلات أعمال أم سجلات مالية أو بيانات شخصية، فإن المؤسسة تحتفظ في سجلاتها وأنظمتها بكميات هائلة من البيانات والمعلومات التي يجب حمايتها.
مخاطر الإلزام غير الفعال وفض النزاعات	تطبق قضايا حوكمة تقنية المعلومات غالباً على أنماط محدودة أو متعددة من الإجراءات التصحيحية ذات الأهمية التي تتخذ عند تنفيذ الإجراءات المناسبة. لذا يجب أن تكون هناك عمليات إدارية نظامية وقوية ومجربة.
مخاطر شح الموارد المالية	في حين أنه من السهل في بعض الأحيان بالنسبة للمختصين أن يقوموا بتطوير خطة علاجية للمخاطر، إلا أن قلة الموارد المالية لدى المؤسسة قد تحول دون استخدام تلك الخطة.

مخاطر الإخفاق في فهم جميع مسؤوليات الأعمال وحاجات أصحاب المصالح	تركز إدارات تقنية المعلومات غالباً على العمليات التشغيلية الخاصة بالبنية التحتية لتقنية المعلومات الخاصة بها ولكنها تخفق في فهم متطلبات ومخاطر العملية الشاملة للمؤسسة، وكذلك تلك التي تخص أصحاب المصالح كالباعة والموردين الرئيسيين.
مخاطر المسؤوليات الائتمانية	على جميع المستويات، تحتاج المؤسسة وعمليات تشغيل تقنية المعلومات (الخاصة بها أو التابعة لها) أن يتذكروا دائماً أن لديهم واجب حماية الأصول والاستثمارات الخاصة بأصحاب المصالح والمقرضين.
مخاطر تحديد الحدود والسلطة	في كثير من الأحيان، نرى أن أنشطة مراقبة ومعالجة المخاطر تمتد لتتجاوز عمليات تشغيل تقنية المعلومات لتصل إلى المؤسسة بأكملها وإلى جميع أصحاب المصالح الآخرين الرئيسيين. لذا فهناك حاجة ماسة للتعرف على السلطات والحدود

تعتبر القواعد والقضايا التنظيمية والتشريعية من العناصر الهامة في العمليات الفعالة لحوكمة تقنية المعلومات. فعلى إدارة المؤسسة مراقبة تلك القواعد واتخاذ الخطوات المناسبة للتأكد على الامتثال بها.

شكل توضيحي (٧-٢)

قضايا الأمن الخاصة بحوكمة تقنية المعلومات

قضايا أمن تقنية المعلومات	أنشطة حوكمة تقنية المعلومات
مخاطر السياسات والإجراءات الأمنية	يجب أن يكون لدى المؤسسة إجراءات قوية لكشف ومنع محاولات الاختراقات والتطفلات الخاصة بأمن تقنية المعلومات. ويجب أن يكون هناك أيضاً فريق مختص ومهاري لمراقبة أمن تقنية المعلومات واتخاذ الإجراءات التصحيحية إذا تطلب الأمر.
قضايا التخطيط لاستمرارية الأعمال	يجب أن يكون هناك عمليات مفعلة لاسترجاع العمليات التشغيلية في حال حدوث اضطرابات غير متوقعة للعمليات التشغيلية والنظم. ويجب فحص هذه النظم بالكامل للمحافظة على الوضع الراهن لتعكس التغيرات الحاصلة في العمليات التشغيلية المؤسسية.

مخاطر البرمجيات الضارة	يجب أن تدرك الإدارة أن جميع الأنظمة هذه الأيام عرضة لمجموعة واسعة ومتطورة باستمرار من البرمجيات الضارة التي لديها المقدرة على تخطي عمليات الكشف عنها بحيث تقوم بتغيير نفسها بمجرد إطلاقها.
متطلبات الكشف الفعال للتسلل وأدوات مراقبة أمن تقنية المعلومات	يجب أن تعمل المؤسسة على إيجاد الأدوات اللازمة لمراقبة جميع الجوانب المتعلقة بأمن تقنية المعلومات، على الصعيدين الداخلي والخارجي، واتخاذ الإجراءات العلاجية الفعالة عند الحاجة.
مخاطر تصنيف أصول تقنية المعلومات	يجب تحديد جميع أصول تقنية المعلومات من البرمجيات والمعدات بشكل مناسب، وتحديد نقاط الضعف الأمني الخاصة بها مع خطط أعمال تصحيحية مجربة ومطبقة ومفعلة.
مخاطر مراقبة أمن تقنية المعلومات	يجب أن تكون هناك أدوات معمول بها لرصد ومراقبة جميع الجوانب المتعلقة بأمن تقنية المعلومات والبدء بالإجراءات الملائمة عند تحديد أي اختراقات أو هجمات أمنية.
مخاطر سياسات التشفير وإدارته	يجب إيجاد سياسات تشفير فعالة واستخدامها عند الضرورة لتحسين الممارسات الخاصة بحوكمة تقنية المعلومات.
مخاطر أمن تقنية المعلومات الخاصة بأصحاب المصلحة	يجب توافر سياسات وأدوات تدريبية لضمان اتباع جميع أصحاب المصلحة المعنيين في المؤسسة لإجراءات مناسبة لأمن تقنية المعلومات.

القضايا الأمنية لحوكمة تقنية المعلومات:

نظراً لترابط العمليات التشغيلية لتقنية المعلومات في المؤسسة على الصعيدين الداخلي والخارجي من خلال الإنترنت والعديد من الروابط الأخرى، فإن أمن تقنية المعلومات يعتبر من القضايا الرئيسية في حوكمة تقنية المعلومات. حيث يدرك العديد من عملاء ومستخدمي تقنية المعلومات أن نظمهم وبياناتهم عرضة لشريحة واسعة من الدخلاء والمتطفلين من الذين تتراوح اهتماماتهم من مجرد التشويش على العمليات التشغيلية لتقنية المعلومات لصالح جهة ما إلى أن تصل إلى حد تخريب النظم والبيانات لتحقيق بعض المكاسب. لذا يعتبر وجود الضوابط الفعالة لأمن تقنية المعلومات من العناصر الهامة في حوكمة تقنية المعلومات.

يجب أن يكون لدى المدير التنفيذي هذه الأيام معرفة عامة عالية المستوى في القضايا الأكثر تأثيراً في أمن تقنية المعلومات والمهمة بالنسبة للحوكمة الفعالة لتقنية المعلومات. فمع أن هناك العديد من القضايا المختلفة في هذا المجال، فإنه يجب على مدير الأعمال أن يفهم التهديدات والمخاطر الخاصة بتقنية المعلومات بل يجب عليه أيضاً البحث عن مساعدة تقنية متخصصة بداخل المؤسسة لتقوم بتطبيق الأنواع الموضحة بالشكل التوضيحي (٧-٢) للعمليات الأمنية الخاصة بحوكمة تقنية المعلومات بشكل أكثر فاعلية.

التهديدات الداخلية والخارجية لحوكمة تقنية المعلومات:

بالإضافة لقضايا حوكمة تقنية المعلومات الأكثر تخصصية، فإن المؤسسة تتعرض لحجم هائل من التهديدات الأمنية الداخلية والخارجية. فقد تمتد التهديدات الخارجية من مجرد أمور أشبه بالهجوم الإرهابي الذي تقوم به إحدى الحكومات الأجنبية المتورطة بقضايا التجسس إلى أن يصل إلى مخاطر تتعلق بالحوسبة السحابية وأكثر. فعلى الرغم من أننا سوف نناقش بعض التهديدات التقنية المتعلقة بالحوسبة السحابية في الفصل التاسع من هذا الكتاب، فإن المؤسسة تواجه هذه الأيام مجموعة واسعة من التهديدات الخارجية التي تهدد مواردها التقنية والعمليات التشغيلية الخاصة بأعمالها أيضاً. لذا يتعين على المدير التنفيذي في هذه الأيام التأكد من أنه تم الاستعانة بأدوات مراقبة ورصد مناسبة وبأشخاص مهرة لمراقبة مثل تلك التهديدات واتخاذ الإجراءات التصحيحية المناسبة.

يمكن مراقبة عمليات حوكمة تقنية المعلومات الخاصة بالتهديدات الداخلية والتحكم بها بشكل أفضل في أغلب الأحيان. ومع أننا لا نعرف مطلقاً الوقت الذي سيقوم به بعض الدخلاء غير المتوقعين بمهاجمة نظم تقنية المعلومات الخاصة بنا، فإننا نستطيع تقليص مخاطر التهديدات الداخلية عن طريق وضع سياسات وإجراءات داخلية قوية تشمل العديد من تلك السياسات والإجراءات التي تمت مناقشتها في هذا الفصل إلى جانب بناء فريق مؤسسي يدرك فيه جميع أصحاب المصالح لأدوارهم ومسؤولياتهم ولتوقعات الإدارة.

كما ذكرنا في هذا الفصل، فإن حوكمة تقنية المعلومات هي المجال الواسع الذي يشمل العديد من المجالات الخاصة بالعمليات التشغيلية المؤسسية وتتجه جيداً إلى ما هو أكثر من مجرد إدارة تقنية المعلومات. وهي أكثر بكثير من الموضوع الساخن الحالي الذي يثير ضجة كبيرة. لذا يجب أن يعمل كبار المديرين التنفيذيين في المؤسسة اليوم جنباً إلى جنب مع الكادر التقني وأخصائيي أمن المعلومات لديهم إلى جانب المدققين الداخليين لتطوير ممارسات قوية لحوكمة تقنية المعلومات. ستقدم الفصول اللاحقة المزيد من المعلومات والنقاشات التي تدور حول تطبيق ممارسات فعالة في حوكمة تقنية معلومات.

ملاحظات:

1. على الرغم من أننا نقدم مجرد ملخص عالي المستوى لمتطلبات قانون SOx ، فإن Robert Moeller, Sarbanes-Oxley Internal Controls: Effective Auditing" (with AS5, CobiT, and ITIL (Hoboken, NJ: John Wiley & Sons, 2008 يقدم الكثير والمزيد من المعلومات.

2. على اعتبار أنها وثيقة عامة، فإنه يمكن العثور على نص القانون في العديد من مواقع الويب. أحد هذه المصادر هي:

<http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf>

3. كأحد مبادئ القانون: حتى لو ظهر انتهاك اصطلاحي للقانون طبقاً لنص القانون، فإن كان تأثيره صغيراً جداً بحيث لا يكون له أي عواقب، فإن انتهاك القانون في هذه الحالة لن يعتد به كسبب كافٍ لاتخاذ أي إجراء، سواء كانت هذه الإجراءات مدنية أم جنائية.

4. Steve Crutchley, "IT Governance Helping Business Survival," www.slideshare.net/khanyasmin/it-governance-consult2comply

5. لمزيد من المعلومات حول إدارة المخاطر المؤسسية وإدارة المخاطر المؤسسية الخاصة بلجنة المنظمات الراعية (COSO ERM) انظر " Robert Moeller's COSO Enterprise " (Risk Management, 2nd ed. (Hoboken, NJ: John Wiley & Sons, 2011.

الفصل الثالث

حوكمة المؤسسات وأدوات الحوكمة وإدارة المخاطر والامتثال GRC

واجهت جميع الشركات التجارية والشركات المساهمة العامة بصفة خاصة منذ نشأتها قضايا تتعلق باحتياجات ومتطلبات الحوكمة. فبالنسبة للعديد من المؤسسات، كانت الإدارة العليا غالباً هي التي تأخذ زمام المبادرة في البداية للقيام بوضع سياسات وقواعد الامتثال للأعمال التي يجب التقيد بها واتباعها من قبل موظفيها وغيرهم. وبالرغم من أن ذلك كان مناسباً بالنسبة للملكيات الفردية الصغيرة أو للشركات المركزية التي كانت موجودة في العصور الماضية، فإن العديد من المؤسسات الكبيرة المتعددة الوحدات تحتاج إلى تسهيلات على نطاق واسع لوضع مثل هذه السياسات والإجراءات، أي أنها بحاجة إلى عمليات حوكمة ذات كفاءة وفعالية.

ستكون الحياة أسهل بكثير بالنسبة لبعض المؤسسات التي تعتمد فقط على قيادة مركزية قوية، رئيس تنفيذي CEO مهيمن، ليفوض ويدير مباشرة تطبيق أي قاعدة من القواعد المطلوبة للحوكمة. من ناحية أخرى، تُواجه الشركات في هذه الأيام على مختلف أماكنها وأحجامها مجموعات متزايدة وبشكل غير مسبوق من القواعد والإجراءات التي تمتد من السياسة المحلية وقوانين السلامة العامة إلى القوانين واللوائح الحكومية التي تصدر على مستوى الولاية والمستوى الوطني، وفي بعض الأحيان على المستوى الدولي، هذا بالإضافة إلى وجود مجموعة كبيرة من القواعد المهنية الهامة. ويتعين على المؤسسة أن تلتزم بتلك اللوائح والقوانين والقواعد على جميع المستويات. وقد يترتب على عدم التزام الشركة بها فرض العديد من العقوبات الجزائية عليها. فكل مؤسسة تحتاج إلى عمليات تضمن التزامها بالقوانين والتشريعات الضرورية.

تكون المؤسسة دائماً عرضة للمخاطر التي تتعلق بعدم فهم أو تفسير القواعد كما ينبغي أو قيامها بانتهاك واحد أو أكثر من القوانين والنظم التشريعية المتعددة. كما يوجد

هناك مخاطر أيضاً تتعلق بعدم قدرة قواعد الحوكمة التي قامت المؤسسة بوضعها على تحقيق النتائج المرجوة، أو أن تواجه المؤسسة بعض الأحداث الخارجية الطارئة الخارجة عن سيطرتها، كحدوث تحولات اقتصادية كبيرة، أو التعرض لهجمات إرهابية أو تحولات اقتصادية كبيرة تؤثر في منطقة عملياتها التشغيلية، أو اندلاع حريق في أحد المرافق الرئيسية للمؤسسة. لذا فهناك حاجة إلى فهم وإدارة جميع تلك المخاطر على مستوى المؤسسة بأكملها.

وعلى الرغم من أن المؤسسة تكون دائماً قلقة إزاء العديد من القضايا المختلفة التي تخص الحوكمة، وإدارة المخاطر، والامتثال. إلا أن السمة الرئيسية لهذا الكتاب أنه قام بجمع كل من هذه المخاوف الثلاثة معاً في سياق تقنية المعلومات وفيما يعرف أيضاً بمبادئ الحوكمة وإدارة المخاطر والامتثال جي آر سي (GRC). وبينما ستناقش الفصول القادمة قضايا أهمية ممارسات الحوكمة المؤسسية وأساسيات إدارة المخاطر وممارسات حوكمة الشركات، سيركز هذا الفصل على أهمية إنشاء مجموعة قوية من مبادئ الحوكمة المؤسسية وإدارة المخاطر والامتثال أو ما يعرف بمبادئ GRC، التي تعد أحد العناصر الهامة في حوكمة تقنية المعلومات.

الطريق نحو مبادئ فعالة للحوكمة وإدارة المخاطر والامتثال GRC:

حتى مطلع القرن الحالي لم يكن أحد من المهنيين قد سمع بمصطلح GRC الشائع بكثرة هذه الأيام. حيث يشير الحرف الأول في هذا المصطلح إلى الحوكمة Governance، ليست حوكمة تقنية المعلومات فحسب، إنما هي حوكمة الأمور المتعلقة بكامل المؤسسة. باختصار، فإن الحوكمة تعني الاهتمام بالأعمال ورعايتها والتأكد من أن جميع الأمور تتم وفقاً للمعايير واللوائح التنظيمية للمؤسسة وكذلك قرارات مجلس إدارة المؤسسة، بالإضافة إلى القوانين والقواعد الحكومية. وهي تعني أيضاً طرح توقعات أصحاب المصلحة بشكل واضح فيما ينبغي عمله كي يكون أصحاب المصالح جميعهم متفقين على الهدف نفسه فيما يخص الكيفية التي تعمل بها المؤسسة.

في حين يشير الحرف R في المصطلح GRC إلى المخاطر Risk. فكل ما نقوم به وكذلك الجوانب المتعلقة بعمليات تشغيل الأعمال قد ينطوي على نوع ما من المخاطرة. فعندما يتعلق الأمر مثلاً بأحد الأشخاص الذي يجري عبر أحد الطرق السريعة، أو الطفل الذي

يلعب بأعواد الثقاب، فمن الواضح هنا أن هذه المخاطر المؤكدة لا يجب قبولها بالمرّة. أما عندما يتعلق الأمر بالأعمال، فإنه ومع ذلك تصبح عوامل المخاطرة طريقة للمساعدة في حماية قيم الأصول الحالية، هذا من جانب، ومن جانب آخر طريقة لخلق قيم جديدة من خلال التوسع الإستراتيجي للشركة أو إضافة منتجات وخدمات جديدة.

وأخيراً يشير الحرف الأخير C في هذا المصطلح GRC إلى الامتثال، أي التقيد أو الالتزام بالعديد من القوانين والتعليمات التي تؤثر في الأعمال والمواطنين اليوم. وأحياناً يقوم الناس بتوسيع مفهوم الامتثال ليشمل أيضاً الضوابط الرقابية Controls، وهذا يعني أنه من المهم وضع ضوابط محددة موضع التنفيذ للتأكد من تحقيق الامتثال. على سبيل المثال، قد نقصد بذلك القيام بمراقبة الانبعاثات الخاصة بأحد المصانع أو التأكد من أن المستندات الخاصة ب وارداته وصادراته سليمة ومطابقة للنظام. أو أنها قد تعني فقط وضع ضوابط جيدة للمحاسبة الداخلية وتطبيق متطلبات تشريعية بطريقة فعالة مثل القواعد الخاصة بقانون SOx التي سبق مناقشتها باختصار في الفصل الثاني من هذا الكتاب. وبضم هذه الحروف جميعها معاً، لا تكون الحوكمة وإدارة المخاطر والامتثال GRC هو ما يجب أن تفعله لرعاية المؤسسة فحسب، إنما هو عبارة عن نموذج أولي يساعد في نمو تلك المؤسسة بأفضل وسيلة ممكنة.

كما ذكرنا في الفقرات التمهيديّة، لم يتم مسبقاً التطرق إلى مبادئ الحوكمة وإدارة المخاطر والامتثال GRC والنظر إليهم على أنها مجموعة موحدة من المبادئ من قبل جميع المؤسسات والشركات على وجه الخصوص. فبمقدار ما كانت المؤسسة تدير أو تهتم بأي من هذه المجالات الثلاثة، بقدر ما كانت غالباً تديرهم معاً بصورة أقل كفاءة عما إذا تمت إداراتهم كمجالات أو اهتمامات منفصلة. إن إدارة المخاطر هنا هي الحالة التقليدية، فقد فكرت المؤسسات بإدارة المخاطر من ناحية التغطية التأمينية، وقامت بإدارة مخاطرها من خلال إدارة التأمين إذ إنها كانت في أغلب الأحيان لا تملك الكثير لتفعله حيال العمليات التشغيلية الأخرى في المؤسسة. وكذلك بالنسبة للامتثال، فنحن بحاجة دائماً للتوافق مع جميع مستويات الإجراءات الموضوعية، متضمناً ذلك القواعد التي تم وضعها للمساعدة في إدارة المؤسسة. ولكن لم يسبق على مر التاريخ أن قمنا بدمج هذه المجالات الثلاثة معاً لتشكّل ما يعرف

مبادئ الحوكمة وإدارة المخاطر والامتثال GRC. فمصطلح GRC اليوم متعارف عليه بشكل متزايد حيث يعكس أسلوباً جديداً تستطيع المؤسسات من خلاله اعتماد نهج متكامل لدمج تلك الجوانب الخاصة بأعمالهم، كما أنه يعكس أسلوباً جديداً يمكن المؤسسات من اعتماد نهج موحد ومتكامل لجميع الجوانب الثلاثة في قالب واحد أثناء إتمام أعمالهم.

بالذهاب إلى أبعد من كونه مجرد اختصار، نجد أنه من المهم تذكر تلك المجالات المحورية لكل من الحوكمة وإدارة المخاطر والامتثال. فكل مجال من هذه المجالات يتكون من أربعة مكونات أساسية لنموذج GRC وهم: الإستراتيجية، والعمليات، والتقنية، والناس.

يوضح الشكل التوضيحي (١-٣) هذه المفاهيم الخاصة بمبادئ GRC، فمبادئ الحوكمة وإدارة المخاطر والامتثال يجب أن تكون محاطة بإحكام لربط هذه المبادئ معاً. ويوضح الشكل أيضاً أن السياسات الداخلية هي العوامل الرئيسية التي تدعم الحوكمة، وأن اللوائح التنظيمية الخارجية هي التي تقود مبادئ وقواعد الامتثال، وأن ما نطلق عليه رغبة المؤسسة في المخاطر يعد أحد العناصر الرئيسية في إدارة المخاطر.

يعتبر مصطلح الرغبة في المخاطر Risk appetite من المصطلحات الجديدة نوعاً ما بالنسبة للعديد من المهنيين في مجال الأعمال وتقنية المعلومات. فهو يشير إلى مقدار ونوع المخاطر التي تستطيع المنظمة متابعتها وتحملها. فعلى سبيل المثال، المستثمر الذي يضارب بأمواله فيما يطلق عليه غالباً بـ "الأسهم ذات الدولار الواحد Penny Stocks" التي تكون محفوفة بالمخاطر، تكون لديه رغبة عالية في المخاطر، في حين أن المستثمر الذي يستثمر أمواله في صناديق سوق المال الآمنة تكون لديه رغبة منخفضة في المخاطر. ويمكن تطبيق السيناريو نفسه على العديد من قرارات الأعمال المؤسسية.

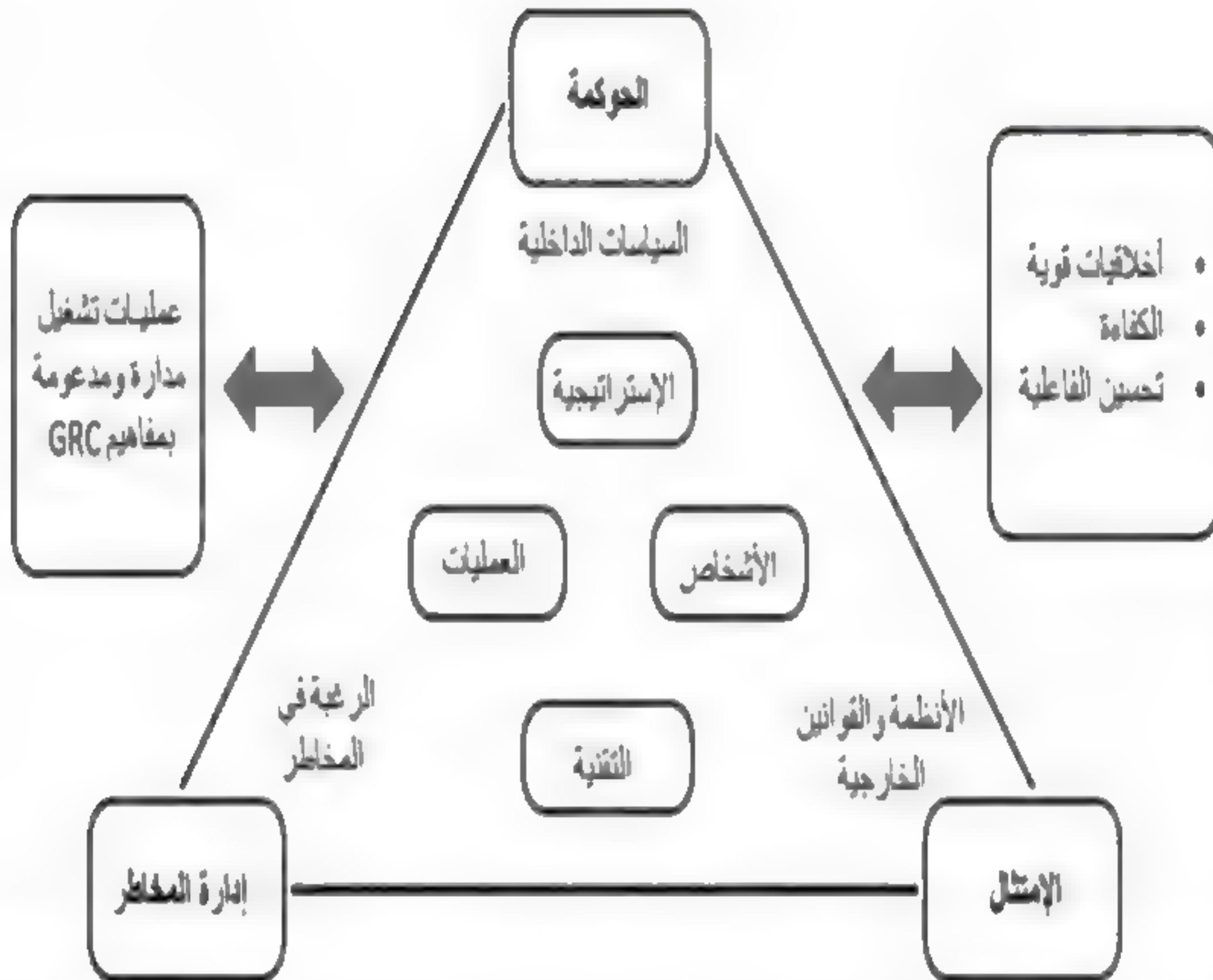
يوضح الشكل التوضيحي (١-٣) أيضاً مكونات الإستراتيجية، والعمليات الفعالة، والتقنيات (بما فيها تقنية المعلومات IT)، والناس داخل المؤسسة للقيام بكل هذا العمل. وعلى الجانب الأيسر للمثلث من الخارج، يوضح الشكل حاجة المؤسسة لاهتمام ودعم الإدارة وأن السلوك الأخلاقي السليم والكفاءة التنظيمية وتحسين الفاعلية تعد من العناصر الأساسية. وستتناول الأقسام التالية من هذا الفصل كل مكون من المكونات الخاصة بنموذج GRC بمزيد من التفصيل، وسنقوم أيضاً بالحديث عن العديد منها في فصول أخرى من هذا الكتاب.

أهمية الحوكمة في نموذج GRC

يجب التفكير بالمبادئ الثلاثة الرئيسية الخاصة بنموذج GRC والداعمة لحوكمة تقنية المعلومات على أنها تيار واحد من المفاهيم المستمرة والمتراصة بحيث لا يكون لأي منها، سواء الحوكمة G أو إدارة المخاطر R أو الامتثال C، أهمية زائدة عن الآخرين. وحيث إن غالبية الفصول القادمة تغطي العديد من جوانب حوكمة تقنية المعلومات، فإننا سنبدأ الحديث هنا عن الجانب الخاص بالحوكمة G في نموذج GRC.

شكل توضيحي (١-٣)

المفاهيم الخاصة بنموذج GRC



حوكمة الشركات أو المؤسسات هو مصطلح يشير بشكل واسع إلى القواعد أو العمليات أو القوانين التي بها يتم تشغيل الأعمال وتنظيمها ومراقبتها. ويمكن أن يشير هذا المصطلح إلى العوامل الداخلية التي تم تحديدها أو تعريفها بواسطة المسؤولين أو أصحاب المصالح أو دستور الشركة، بالإضافة إلى القوى الخارجية كمجموعات المستهلكين والعملاء واللوائح التنظيمية الحكومية.

نزولاً من المستويات العليا للشركة ووصولاً إلى العديد من المجالات الخاصة بالعمليات التشغيلية في الشركة، يمكننا تعريف حوكمة المؤسسات على أنها المسئوليات والممارسات التي يتم تنفيذها من قبل مجلس الإدارة، والإدارة التنفيذية العليا، وجميع المستويات الخاصة بالإدارة الوظيفية العليا، بهدف توفير توجه إستراتيجي، والتأكد من أن الأهداف الموضوعية قد تم تحقيقها، والتأكد من أن المخاطر قد تمت إدارتها بالأسلوب المناسب، وفحص ما إذا كانت موارد المؤسسة قد تم استخدامها بشكل معقول. فالحوكمة في الواقع تشير إلى عملية وضع القواعد والإجراءات في جميع مستويات المؤسسة، وتوصيل هذه القواعد إلى المستويات المناسبة من أصحاب المصلحة، ومراقبة الأداء وفقاً لتلك القواعد، ومن ثم إدارة المكافآت والعقوبات بناء على الأداء أو الامتثال النسبي لتلك القواعد.

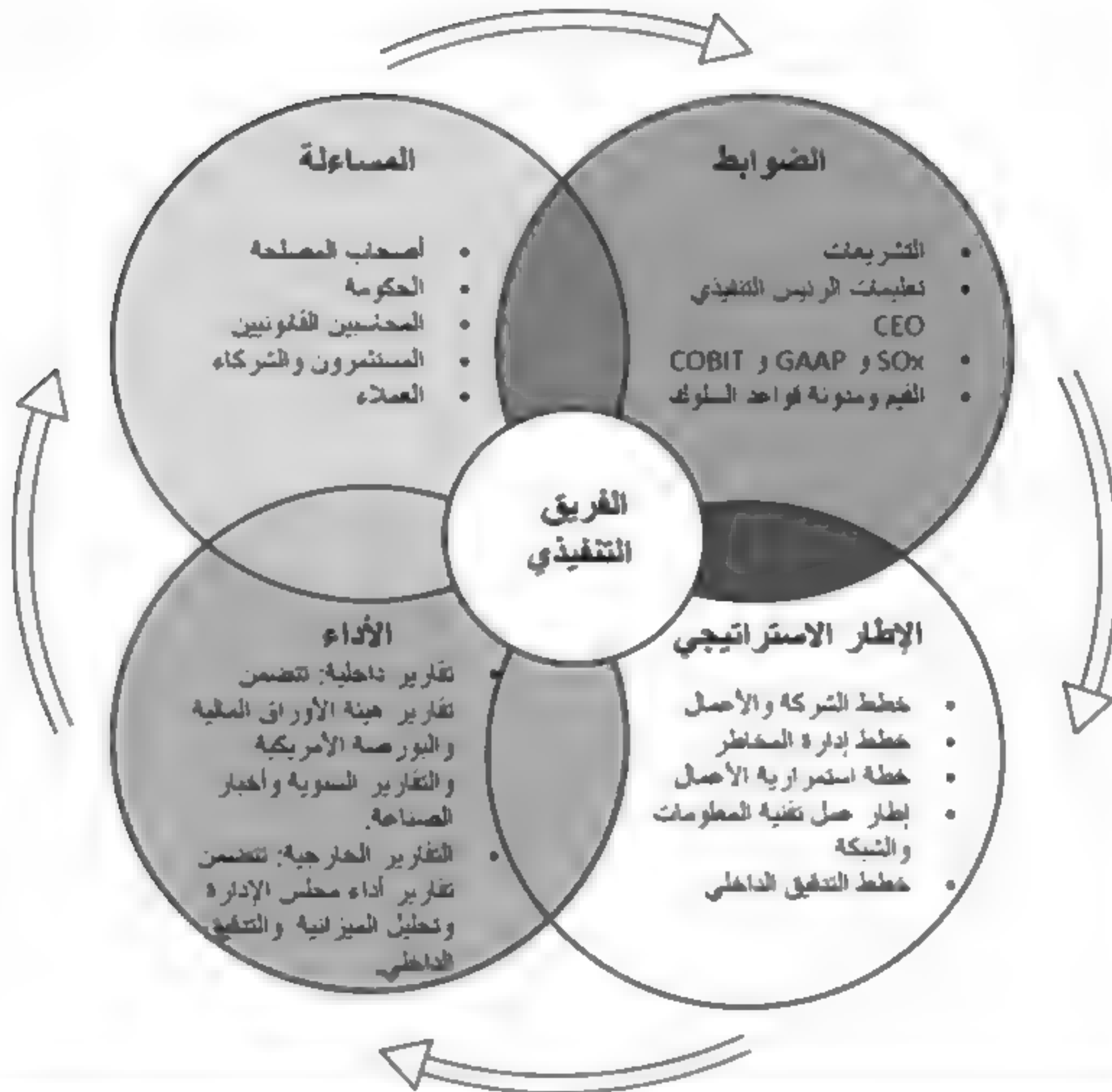
توفر مجموعة مبادئ حوكمة الشركات أو المؤسسات المعرفة بشكل جيد والتي يتم إنفاذها بأسلوب جيد، على الأقل من الناحية النظرية، الأعمال التي تصب في مصلحة كل فرد مهتم بضمان أن تلتزم المؤسسة بالمعايير الأخلاقية المعتمدة واتباع أفضل الممارسات، بالإضافة إلى اللوائح والقوانين والمعايير الرسمية المناسبة. لقد لاقت قضايا حوكمة الشركات المزيد من الاهتمام في السنوات الأخيرة نتيجة الفضائح المدوية الناجمة عن سوء استخدام السلطة في الشركات، وسوء التقديرات المالية، وفي بعض الحالات، ممارسة أنشطة جنائية من قبل مسئولي الشركة. إن وضع أحكام قضائية، سواء كانت مدنية أم جنائية، لإدانة الأفراد الذين يقومون بأعمال لا أخلاقية وغير قانونية باسم الشركة يعد جزءاً مكملًا ومتمماً للنظام الجيد والفعال الخاص بحوكمة الشركات.

وعلى الرغم من أننا كثيراً ما نقوم بوصف جميع مفاهيم الحوكمة الخاصة بالمؤسسات أو الشركات باستخدام القليل من الفقرات القصيرة أو باستخدام صور واحدة، فإن الشكل التوضيحي (٢-٣) يعرض مجالات تتعلق بمفاهيم الحوكمة المؤسسية باستخدام مجموعة تنفيذية في وسط الشكل، كما يوضح الشكل بعض التداخل أو التشارك الموجود بين هذه المفاهيم والمسؤوليات المرتبطة بها من أجل تأسيس كل من الضوابط والإطار الإستراتيجي للأعمال وتحسين الأداء وفرض المساءلة أو المحاسبة. كما يعرض الشكل التوضيحي (٢-٣) أيضاً بعض المفاهيم الرئيسية التي تندرج تحت كل مجال من مجالات المسؤولية تلك. فمثلاً بالنسبة للإطار الإستراتيجي للأعمال، يوجد بها عدة عناصر أو مفاهيم مهمة كأنشطة التخطيط والأعمال المؤسسية وإدارة المخاطر واستمرارية الأعمال وتقنية المعلومات والشبكات والتدقيق الداخلي.

تم تضمين الحوكمة، وهي جزء رئيسي في نموذج مبادئ GRC، في العديد من الفصول اللاحقة والتي تتحدث عن قضايا معينة في حوكمة تقنية المعلومات، ونخص بالذكر هنا كلاً من الفصل الثامن الذي يتحدث عن إدارة المخاطر، والفصل الثامن عشر الذي تناول الحديث عن حوكمة تقنية المعلومات. ويركز الفصل الثامن عشر أيضاً على مسائل متعلقة بتقنية المعلومات وإستراتيجيات الأعمال وعمليات الحوكمة.

شكل توضيحي (٣-٢)

عناصر حوكمة GRC



عنصر إدارة المخاطر في نموذج GRC:

إن الهدف الرئيسي لهذا الكتاب هو تقديم مفاهيم حوكمة تقنية المعلومات إلى مسئولي الأعمال التنفيذيين. فمن الضروري أن يكون هناك مجموعة قوية من مكونات ومبادئ الحوكمة وإدارة المخاطر والامتثال GRC على مستوى المؤسسة بأكملها، ويعد البرنامج الفعال لإدارة المخاطر أحد العناصر الرئيسية لمبادئ GRC في المؤسسة. وسيتم الحديث

بمزيد من التفصيل عن أساسيات إدارة المخاطر وأمن تقنية المعلومات في كل من الفصل الثامن والعاشر من هذا الكتاب، حيث يجب أن تصبح إدارة المخاطر جزءاً من الثقافة العامة للمؤسسة ابتداءً من مجلس الإدارة وكبار المسؤولين نزولاً إلى جميع أنحاء المؤسسة. هناك أربع خطوات مترابطة في العمليات الفعالة لإدارة المخاطر المؤسسية وفقاً لنموذج GRC كما هو واضح في الشكل التوضيحي (٣-٣) وهي:

١- **تقييم المخاطر والتخطيط لها:** قد تتعرض المؤسسات إلى مستويات متعددة من المخاطر، سواء كانت قضايا عالمية تتراوح بين أزمات الاقتصاد المحلي أم أزمات العملة، إلى عوامل المنافسة في سوق المنتجات وحوادث اضطرابات في العمليات التشغيلية المحلية نتيجة سوء الأحوال الجوية. وهنا لا يمكننا تعريف كل نوع من أنواع المخاطر التي قد تؤثر في المؤسسة والتخطيط لها، إلا أنه ينبغي أن يكون هناك تحليل مستمر لمختلف المخاطر المحتملة التي قد تواجه المؤسسة.

٢- **تحديد وتحليل المخاطر:** بدلاً من التخطيط فقط لاحتمالية وقوع بعض المخاطر، هناك حاجة ماسة إلى المزيد من التحاليل التفصيلية التي تمكننا من معرفة احتمالية وقوع هذه المخاطر القادمة ومعرفة مدى تأثيراتها المحتملة أيضاً. كما أن هناك حاجة أيضاً لقياس الآثار المترتبة على تلك المخاطر المحددة، وذلك لتحديد إستراتيجيات للعمل على التخفيف من آثارها في حال وقوع أحداث تلك المخاطر. يشير التخفيف هنا إلى تقدير أفضل وسيلة لإدارة المخاطرة أو استبعادها. كما يجب أيضاً تحديد العوامل النهائية المرتبطة بتلك المخاطر. وستصبح المخاطر المحددة أكثر أهمية إذا استطعنا تحديد التكاليف الإجمالية التي ستحملها الشركة إذا وقعت تلك المخاطر المحددة.

٣- **توظيف وتطوير إستراتيجيات الاستجابة للمخاطر:** يجب أن تضع المؤسسة خططاً وإستراتيجيات واضحة لاستعادة العمليات التشغيلية الطبيعية الخاصة بها والتعافي من أحداث المخاطر التي يمكن أن تحدث، ويجب أن يتم ذلك بشكل أساسي بالتوازي مع تحديد تلك المخاطر. وقد يشتمل ذلك على تحليل الفرص المتعلقة بالمخاطر. فعلى سبيل المثال، إذا كان لدينا أحد المخاطر المحددة سلفاً تخص

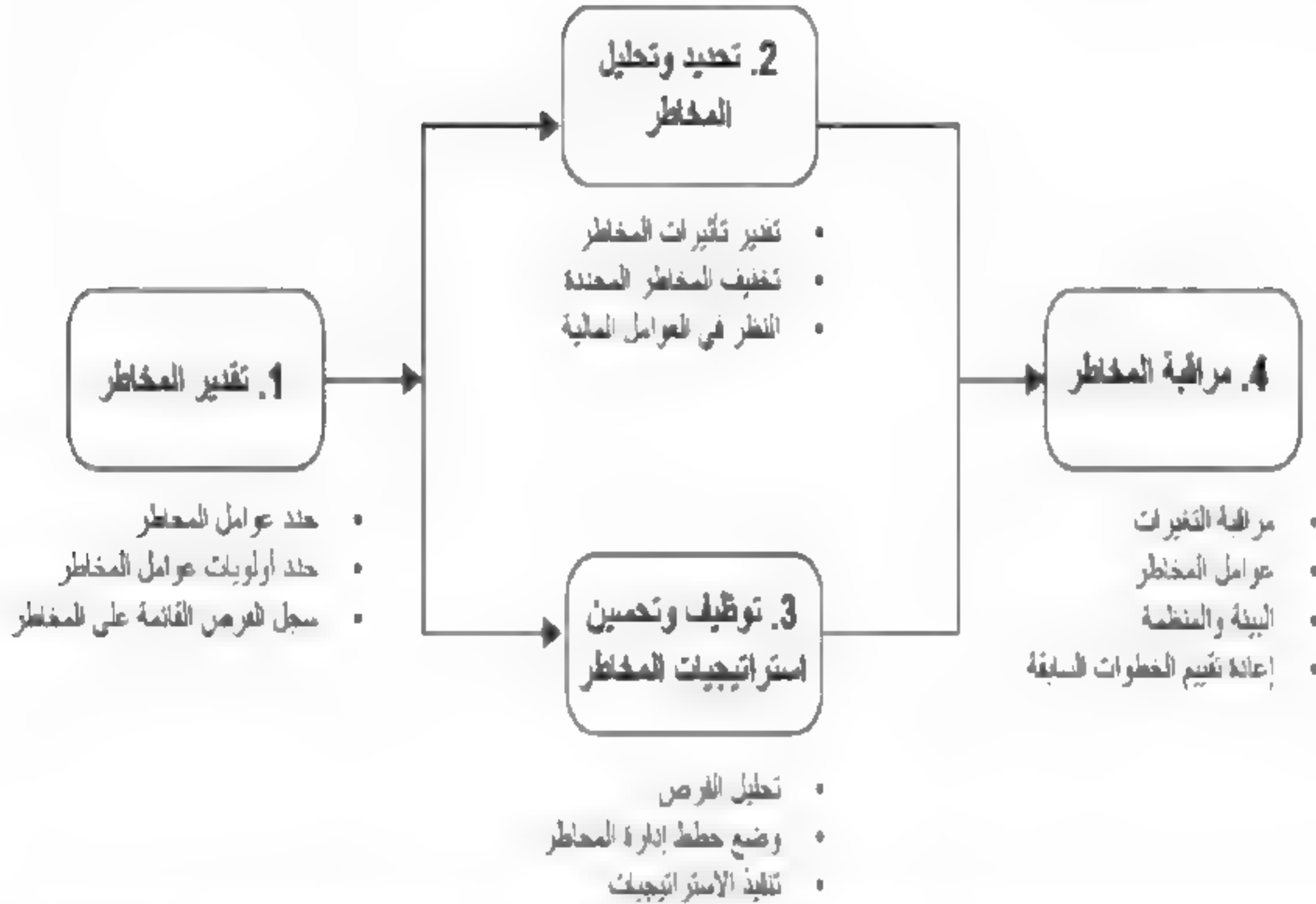
معدات إنتاج قديمة في أحد المصانع والتي ربما تتوقف عن الإنتاج، فقد تكون هذه فرصة للتخلي عن خط الإنتاج هذا وتركيب معدات جديدة تستخدم تقنيات حديثة، أو حتى من الممكن أن تكون فرصة لنقل المصنع إلى موقع أحدث أو موقع بديل للموقع الحالي.

٤- **متابعة المخاطر:** يجب أن تكون هناك أدوات وتجهيزات معمول بها لرصد جميع المخاطر المحددة والجديدة أيضاً والتي من الممكن حدوثها، مثل وضع جهاز إنذار حريق للكشف عن الدخان. وبالرغم من أن معظم عمليات مراقبة المخاطر تحتاج إلى سلسلة ممتدة من التقارير الخاصة، وإلى معايير معمول بها وقابلة للقياس، وإلى إدارة موارد بشرية يقظه، فإن الفكرة هنا هي أن تكون سابقاً أو متقدماً بخطوة وتعاود الدخول في تلك الخطوات السابق ذكرها لإدارة المخاطر إذا اقتضى الأمر ذلك.

يجب أن تعمل إدارة المخاطر على إيجاد قيمة وأن تكون جزءاً متمماً للعمليات التنظيمية. كما يجب أن تكون جزءاً من عمليات صنع القرار وأن تكون مصممة بأسلوب منهجي ومنظم لمعالجة الشكوك أو الأحداث المبهمة التي يمكن أن تواجه المؤسسة، وذلك بالاعتماد على أفضل المعلومات المتاحة. هذا بالإضافة إلى أنه يجب أيضاً أن تكون تلك العمليات الخاصة بإدارة المخاطر مرنة وتكرارية ومستجيبة للتغيرات من خلال القدرات الخاصة بالتطويرات والتحسينات المستمرة.

شكل توضيحي (٣-٣)

نظرة عامة على إدارة المخاطر



نموذج GRC وامتثال المؤسسة:

الامتثال هو عملية الالتزام أو التقيد بالإرشادات أو بالقواعد الموضوعة من قبل الهيئات الحكومية، أو المجموعات المختلفة لوضع المعايير، أو السياسات الداخلية للشركة. ويعد الالتزام أو التقيد بمتطلبات الامتثال أحد التحديات بالنسبة للمؤسسة وأصحاب المصالح لديها، وذلك للأسباب التالية:

- طرح لوائح تنظيمية جديدة بصورة متكررة: بالنظر إلى الولايات المتحدة الأمريكية هناك العديد من الوكالات، كوكالة حماية البيئة مثلاً، والتي تقوم وبشكل منتظم بإصدار قواعد جديدة يمكن أن تؤثر بشكل كبير في العديد من المؤسسات رغم اختلاف أغراضها

الأساسية. فالتحدي بالنسبة للشركات هنا هو متابعة تلك القواعد الجديدة لمعرفة أي من هذه القواعد يمكن أن ينطبق عليها.

- وجود قوانين غامضة وبحاجة إلى تفسير: وبالنظر مرة أخرى إلى الولايات المتحدة الأمريكية على سبيل المثال، فقد أقر الكونجرس الأمريكي مشروع قانون إصلاح الرعاية الصحية في عام ٢٠١٠، والمعروف باسم أوباما كير (Obamacare)، والذي تمت صياغته من قبل هيئة من أعضاء الكونجرس وطباعته في عدة آلاف من الصفحات التي تغطي قضايا وقواعد لم تتم قراءتها قط، حتى من قبل المشرعين لهذا القانون، ناهيك عن إمكانية فهمها. حتى هذه الأيام وللسنوات قادمة سنظل ننظر إلى هذه القواعد ونحاول تفسير المعاني الحقيقية المقصودة منها. ويمكننا أيضاً الحديث عن قانون دود فرانك Dodd-Frank للإصلاح المالي سنة ٢٠١١ كمثال آخر مشابه للمثال السابق. فهو عبارة عن قانون معقد جداً لتنظيم المجال المالي، ويحتوي هذا القانون على العديد من القواعد الإدارية التي لم تكن قد نشرت بعد حتى وقت إعداد هذا الكتاب. وقد يكون امتثال المؤسسة لتلك القواعد أمراً في غاية الصعوبة.

- لا يوجد إجماع على أفضل الممارسات في الامتثال: إن القواعد مليئة باللوائح القانونية التي تنص على أمور مثل: "جميع المعاملات التي تتم لأبد أن تكون مدعومة بالإيصالات". فهل يشترط هذا القانون استخدام إيصالات في المعاملات التي تقل قيمتها عن ١\$ أو عن ٢٥\$ أو عن أي قيمة أخرى؟ فلا يوجد هناك أي إرشادات خاصة لتلك القاعدة ويستطيع كل شخص أن يفسرها كما يحلو له.

- كثرة تداخل اللوائح التنظيمية مع بعضها البعض: فغالباً ما تقوم الولايات المتحدة الأمريكية والحكومات المحلية الموجودة في مختلف الولايات بإصدار قوانين تغطي المجالات نفسها، إلا أن لها متطلبات مختلفة. ويتم البت في هذه الاختلافات عادة في النهاية داخل ساحات المحاكم. وتبقى قضية الامتثال أحد التحديات إلى أن يتم الفصل في هذه الأمور.

- تغير اللوائح التنظيمية بصفة مستمرة: فغالباً ما تقوم الهيئات التنظيمية وبشكل مستمر ودوري بتغيير قوانينها أو التفسيرات المتعلقة بقوانينها، الأمر الذي يجعل الامتثال تحدياً كبيراً.

لا بد من النظر إلى قضية امتثال المؤسسة على أنها عملية مستمرة وليست مشروعاً ينفذ مرة واحدة فقط. فضلاً عن أن متطلبات الامتثال مستمرة في صدارة جداول الأعمال الخاصة بالمؤسسات، نظراً لأنه يجري محاسبة المؤسسات على وفائها بالتفويضات الكثيرة المتعلقة بأسواقها الخاصة أو مجالات عملياتها التشغيلية.

هذا بالإضافة إلى أن المؤسسات قد تكون مطالبة أيضاً بمعالجة التشريعات التي تتم عبر الأنشطة الصناعية، كمعيار أمن بيانات بطاقات الدفع Payment Card Industry Data Security Standard (PCI DSS) وغيرها من القواعد التي سنتحدث عنها في الفصل الحادي عشر من هذا الكتاب، بالإضافة إلى القضايا الأخرى الخاصة بحوكمة وإدارة تقنية المعلومات التي تم طرحها في الفصل الخامس عشر من هذا الكتاب. ببساطة يمكن القول بأن اتساع دائرة وتعقيد القوانين واللوائح المتعلقة بالامتثال قد تتسبب في وجود تحديات للعديد من المؤسسات على مر السنين. تحتاج المؤسسات إلى الإقبال على مبادئ الامتثال الخاصة بنموذج GRC من منظور أكثر إستراتيجية، الأمر الذي قد يساعدها على الانتقال إلى ما هو أبعد من مجرد الوفاء والالتزام بالقوانين والمعايير والمبادئ المفروضة بل إلى تحقيق فوائد تجارية ملموسة وحقيقية من مجمل استثماراتها في البنية التحتية.

يتخلل نطاق الامتثال العديد من الأنشطة وعمليات التشغيل داخل المؤسسة. ويوضح الشكل التوضيحي (٣-٤) بعض المسائل التي يجب على المؤسسة أن تأخذها بعين الاعتبار عند قيامها بتحديد النطاق والنهج الذي ستستخدمه من أجل تحقيق مبادئ الامتثال الخاصة بنموذج GRC. لذا يجب على المؤسسة ألا تهمل أياً من هذه القواعد وأن تكون دائماً على علم بوجودها. غير أن اتباع نهج منتظم ومتناغم لاستخدام الإمكانيات والتقنيات الداعمة التي تقودها مبادئ الامتثال في جميع أنحاء المؤسسة يمكن أن يسهم في منح المؤسسة العديد من الفوائد المحتملة التالية:

- **المرونة:** تعد الأنظمة التشريعية الجديدة الصادرة عن الهيئات المصrch لها بإصدارها، والتغيير المستمر للقوانين الحالية، واحدة من الصعوبات المتعلقة بعملية الامتثال. فمن خلال إدارة مبادرات الامتثال بشكل مركزي عبر بنية الامتثال على مستوى المؤسسة، يمكن للمؤسسة أن تتكيف وبسرعة أكبر مع هذه التغييرات.

- انخفاض التكلفة الإجمالية لحيازة الامتثال: قد يكون هناك تأثير إيجابي في الاستثمارات جراء العديد من الأنظمة التشريعية. فعلى سبيل المثال، الاستثمار في نظام إدارة قواعد البيانات والسجلات كان نتيجة مطالبة العديد من اللوائح التنظيمية التشريعية للقيام بالاحتفاظ بالوثائق والسجلات الرسمية. الأمر الذي قد يقابل باستثمار فردي في إحدى الوسائل الخاصة بقاعدة بيانات المحتوى ونظام إدارة السجلات.

- الميزة التنافسية: قد تسمح بنية الامتثال الواسعة والمتناغمة للمؤسسة بأن تكون أكثر إدراكاً وتحكماً بعملياتها، الأمر الذي قد يمكنها من سرعة ودقة الاستجابة والتكيف مع ضغوطات الامتثال الداخلية أو الخارجية. هذا بالإضافة إلى احتمالية أن تحتوي بعض الأنظمة التشريعية على العديد من الفوائد التجارية الهامة والملموسة، وذلك من خلال متطلبات كتخفيض الحد الأدنى من رأس المال والتي يمكن تفعيلها من خلال بنية الامتثال على مستوى المؤسسة بأكملها.

تساعد العمليات الفعالة للامتثال الخاصة بنموذج GRC المؤسسة أن تقوم بتغيير عمليات تشغيل الأعمال لديها والحصول على تبصر وإمكانية توقع أعمق من خلال المعلومات التي تخص الأعمال عندما تقوم بمعالجة المتطلبات المدفوعة تنظيمياً. ولعل أهم العوامل المحركة للأعمال هنا هي القدرة على تحسين إدارة أصول المعلومات وإثبات الامتثال للالتزامات التنظيمية والقانونية والحد من مخاطر الدعاوى القضائية ومن تكاليف التخزين والاكتشاف وإثبات مساءلة الشركات.

شكل توضيحي (٣-٤)

اعتبارات المؤسسة الخاصة بنطاق أنشطة الامتثال الخاصة بها

النطاق الخاص بمجال الامتثال	دائرة الاهتمام
الاستراتيجية	• يجب أن تحدد المؤسسة اللوائح التنظيمية الأكثر ارتباطاً بأعمالها أثناء تطوير خطتها الإستراتيجية.
	• استدامة الامتثال يجب أن يكون جزءاً أساسياً ومتمماً في أي خطة إستراتيجية للامتثال.
المنظمة	• يجب وضع الهيكل التنظيمي لتلبية متطلبات (أو مقاصد) محددة لكل تشريع من التشريعات (فعلى سبيل المثال، يوصي قانون SOX ألا يكون رئيس مجلس الإدارة هو نفسه الرئيس التنفيذي)
العمليات	• يجب توثيق وممارسة العمليات الرئيسية للامتثال.
	• يجب أن تتم عمليات التدقيق والمراجعة للتأكد من أن العمليات الموثقة يتم استخدامها بشكل فعال لمعالجة متطلبات الامتثال.
التطبيقات والبيانات	• التطبيقات يجب أن تُصمم وتُنفذ وتُفحص بشكل دوري لضمان دعمها لمتطلبات كل قانون تشريعي.
	• يجب حماية البيانات ومعالجتها بشكل صحيح طبقاً لكل قانون تشريعي.
التسهيلات (المرافق)	• يجب أن تكون جميع التسهيلات مصممة ومتاحة لتلبية احتياجات كل قانون تشريعي (فعلى سبيل المثال، قد تتطلب بعض القوانين التشريعية بأن تكون السجلات متاحة بكل سهولة وسرعة خارج الموقع).

أهمية ممارسات ومبادئ نموذج GRC الفعالة:

تحتاج المؤسسة إلى الاعتماد على ممارسات وإجراءات قوية لكل من عمليات الحوكمة وإدارة المخاطر والامتثال بهدف إيجاد برنامج فعال لنموذج GRC. فعلى الرغم من أن معظم الفصول اللاحقة تركز على عمليات حوكمة تقنية المعلومات، إلا أننا يجب ألا ننسى أبداً الأهمية الكبرى للعمليات القوية لكل من الحوكمة وإدارة المخاطر والامتثال والتي تقوم بدعم كل من حوكمة تقنية المعلومات وغيرها من عمليات التشغيل في المؤسسة. سيتم ذكر مبادئ وممارسات نموذج الحوكمة وإدارة المخاطر والامتثال GRC في جميع الفصول القادمة التي تركز أكثر على قضايا محددة في المخاطر والحوكمة.

ومثالاً على ذلك، سيناقدش الفصل الخامس عشر من هذا الكتاب أهمية تطبيق نظم متكاملة لحوكمة وإدارة تقنية المعلومات. فهو يناقش الأدوار والمسؤوليات المطلوبة لكل من الأشخاص والإدارات للوصول إلى حوكمة فعالة. كما يحدد أساليب التواصل مع المستويات المختلفة لقواعد الحوكمة. وكذلك الأمر بالنسبة للفصل التاسع عشر من هذا الكتاب، الذي ينظر إلى دور التدقيق الداخلي في حوكمة تقنية المعلومات المؤسسية. حيث يوضح هذا الفصل النهج المتبع في تقييم المخاطر والتخطيط لها من قبل إدارة التدقيق الداخلي لكي تقوم بتحديد قضايا الامتثال الأكثر أهمية بالنسبة لها، ولكي تقوم أيضاً بإيصال تلك القواعد والمبادئ الخاصة بالامتثال للجميع، ولكي تقوم بعد ذلك بمراقبة الأداء الحقيقي لعملية الامتثال في المؤسسة. فهذا الفصل يناقش كيف يمكن للقانون والتدقيق الداخلي أن يساعدوا المؤسسة على تحقيق الامتثال.

على الرغم من أن البرامج القوية لحوكمة تقنية المعلومات تعد من الأمور الهامة للغاية، فإنها يجب أن تكون أيضاً مدعومة من قبل برامج الحوكمة وإدارة المخاطر وكذلك الامتثال الكلي لنموذج GRC. كما يجب على المؤسسة أن تركز على العديد من أنشطتها على مبادئ برنامج GRC بشكل قوي. قدم هذا الفصل بعض المفاهيم المؤسسية العالية المستوى الهامة لبرنامج GRC. فهذه المفاهيم يجب أن تكون من المكونات الأساسية لعمليات حوكمة تقنية المعلومات.

الجزء الثاني

أطر عمل لدعم حوكمة فعالة لتقنية المعلومات

الفصل الرابع

حوكمة تقنية المعلومات ونظم الرقابة الداخلية طبقاً للجنة المنظمات الراعية (كوسو- COSO)

إن الحاجة إلى نظم رقابة داخلية قوية وفعالة تعد عنصراً أساسياً في حوكمة تقنية المعلومات لأي مؤسسة. فقد ظهرت الحاجة إلى إنشاء رقابة داخلية وتقييمها منذ الأيام الأولى لظهور نظم التدقيق، بل كانت أيضاً قضية مهمة تعود إلى الأيام الأولى لنشأة نظم تدقيق تقنية المعلومات. وفي حين ظهرت تعريفات عديدة لنظم الرقابة الداخلية في السنوات الماضية فإن هناك تعريفاً عاماً جيداً يتناسب مع حوكمة تقنية المعلومات مفاده أن الرقابة الداخلية عبارة عن "عملية تتأثر بمجلس إدارة كيان ما وإدارته وغيرهم من الأفراد في ذلك الكيان، ويكون الهدف من تصميمها الحصول على تأكيد معقول حول تحقيق الأهداف المنتظرة من فاعلية العمليات وكفاءتها وموثوقية وضع التقارير المالية للمؤسسة ونظم وعمليات تقنية المعلومات داخل المؤسسة، كل ذلك مع الالتزام بالقوانين واللوائح". ويتشابه هذا التعريف مع التعريف المعروف الموضوع من قبل اللجنة الأمريكية للمنظمات الراعية (COSO)، وهي هيئة مهمة تقدم توجيهات تتعلق بنظم الرقابة الداخلية التي سنناقشها لاحقاً في هذا الفصل.

يتحمل مديرو المؤسسة مسئولية تنفيذ عمليات الرقابة الداخلية وإدارتها، في حين يعمل مدققوهم أطرافاً مستقلة تقوم بمراجعة اختبارات نظم الرقابة الداخلية وإجرائها بالإضافة إلى رفع تقارير إلى الإدارة والأطراف الأخرى حال بلوغهم حد الكفاية. ويضم مدققو الرقابة الداخلية كلاً من المدققين الداخليين والخارجيين، حيث يتبنى المدققون الخارجيون في الولايات المتحدة معايير التدقيق الخاصة بالمعهد الأمريكي للمحاسبين القانونيين (AICPA). وعموماً يشترك المدققون الداخليون في اتباع إرشادات معهد المدققين الداخليين (IIA)، وهي منظماتهم المهنية الدولية التي سيتم التطرق إليها في الفصل التاسع عشر من هذا الكتاب.

لكل من منظمتي التدقيق هاتين إرثٌ يعود إلى أيام استخدام الورقة والقلم الرصاص في التدقيق وحتى قبل ما نشهده اليوم من الاستخدام السائد والاعتماد على عمليات تقنية المعلومات ونُظُمها. كما قامت جمعية تدقيق ومراقبة نظم المعلومات (ISACA) والمتخصصون لديها في مجال تدقيق تقنية المعلومات بتلبية جزء كبير من الحاجة إلى وجود نظم رقابية داخلية فعالة.

يضطلع مدققو تقنية المعلومات بأدوار التدقيق الداخلي والخارجي، على الرغم من أن غالبية المهنيين هنا يعملون مدققين داخليين لمؤسساتهم.

ومتابعة منا للمناقشة التي أجريناها في الفصل الثاني عن حوكمة تقنية المعلومات وقوانين ساربينز-أوكسلي (SOX)، فإننا نقدم في هذا الفصل ما يعرف بإطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) كما يلخص عمليات حوكمة تقنية المعلومات المرتبطة بهذه اللجنة (COSO) في مؤسسات أعمال عصرنا الحاضر. إن كلاً من نظم الرقابة الداخلية الخاصة بلجنة المنظمات الراعية (COSO) وقوانين ساربينز-أوكسلي (SOX) التي ناقشناها في الفصل الثاني بدأت مجرد قوانين توجيهية لنظم الرقابة الداخلية المعمول بها في الولايات المتحدة، غير أنها قد لاقت قبولاً الآن في جميع أنحاء العالم. فقد كان كل منهما في الأساس عبارة عن توجيهات عامة لمراجعة الشئون المالية وعمليات التشغيل وتقبل التطبيق تماماً في بيئات حوكمة تقنية المعلومات.

إن فهم إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) واستخدامه يعد أمراً هاماً لوضع عمليات فعالة لحوكمة تقنية المعلومات. ورغم أن هذه القواعد والإجراءات ترجع أصولها إلى إعداد التقارير المالية وتدقيقها، فإنه في عالم اليوم الذي يركز على تقنية المعلومات تجد أن نظم أو ضوابط الرقابة الداخلية الخاصة بلجنة المنظمات الراعية (COSO) تعتبر أدوات هامة في حوكمة تقنية المعلومات. وتلك هي القواعد التي تتبناها المؤسسات للتأكيد أو التصديق للجهات الرقابية بأن منظماتهم تتبع نظاماً رقابية داخلية فعالة وأنها تعمل وفقاً لهذه القواعد الجديدة.

أهمية أنظمة الرقابة الداخلية الفعالة ولجنة المنظمات الراعية (COSO):

تعد نظم الرقابة الداخلية أحد المفاهيم الأساسية وأكثرها أهمية ويجب على كبار المديرين والمهنيين على جميع المستويات أن يفهموها، حيث يقوم المهني بوضع نظم الرقابة الداخلية واستخدامها في حين يقوم المدققون بمراجعة النظم والعمليات التشغيلية والتقنية والمالية واختبارها بهدف تقييم ما لديها من نظم رقابة داخلية. ومع أن كلا من المدققين الداخليين والخارجيين لديهم أهداف متباينة فإن معظم مرجعياتنا في هذا الفصل تنطبق على كبار المديرين الذين تقع على عاتقهم مسئولية رئيسية لفهم قضايا حوكمة تقنية المعلومات وتقييم نظم الرقابة الداخلية ذات الصلة بتقنية المعلومات.

وعلى الرغم من وجود تعريفات كثيرة مختلفة نسبياً لنظم الرقابة الداخلية في الماضي، فإن إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) الذي سناقشه في الأجزاء التالية يقدم تعريفاً مناسباً لكبار المديرين، فهذا التعريف يقر بأن الرقابة الداخلية لا تقتصر فقط على الأمور المالية والمحاسبية بل تتعدى هذا الحد لتشمل جميع عمليات المؤسسة. ولأن تقنية المعلومات تمثل أيضاً جزءاً لا يتجزأ من جميع عمليات الأعمال، فإن نظم الرقابة الداخلية ذات الصلة بتقنية المعلومات تعد جزءاً رئيسياً من فهمنا الشامل لنظم الرقابة الداخلية. ويمكن الحكم بأن المؤسسة، في صورة وحدة أو عملية، يكون لها نظم رقابة داخلية جيدة إذا كانت (١) تحقق مهمتها المعلنة بطريقة أخلاقية، (٢) تعطي بيانات دقيقة وموثوقة بها، (٣) تتوافق مع القوانين المعمول بها ومع سياسات المؤسسة، (٤) توفر استخدامات فعالة واقتصادية لمواردها، وأخيراً (٥) توفر حماية مناسبة للأصول. يتحمل جميع أعضاء المؤسسة المسئولية عن نظم الرقابة الداخلية في مجال عملياتهم التشغيلية وكذا عن تشغيلها على نحو فعال.

وعلى الرغم من - أو بسبب - هذا التعريف الفصفا لنظم الرقابة الداخلية، فإننا نجد أن كثيراً من المهنيين كانت لديهم مشاكل في فهم مفاهيم الرقابة الداخلية وتطبيقها تماماً. وبالنظر إلى تعريفنا هذا بصورة مختلفة بعض الشيء نجد أن مفهوم الرقابة الداخلية ودعم عمليات الرقابة تعود إلى الإجراءات الآلية والأعمال الورقية الأساسية التي كانت تتم بشكل متكرر في جميع العمليات التجارية اليومية. وتعد أعمال الرقابة ضرورية للأنشطة داخل

وخارج مؤسسات اليوم، وأن العديد من المفاهيم والمبادئ الأساسية تكون متماثلة بغض النظر عن مكان تطبيق الرقابة. وتقدم السيارة بعض أمثلة على الرقابة الأساسية، فعند الضغط على المُسرّع - ضابط السرعة - فإن السيارة تسير بشكل أسرع وعند الضغط على المكابح - وهو ضابط آخر للسرعة - فإن السيارة تسير ببطء أو تتوقف، وعندما تُدار عجلة القيادة فإن السيارة تقوم بالدوران، وبذلك يتحكم السائق في السيارة ويمثل كل من هذه الأجزاء الثلاثة النظام الأساسي للرقابة الداخلية بالسيارة. وإذا لم يقم السائق باستخدام المُسرّع أو المكابح أو عجلة القيادة أو إذا استخدمها بشكل غير ملائم فإن السيارة ستعمل خارج نطاق السيطرة.

وبتوسيع هذا المفهوم قليلاً، فإننا نجد أن إشارات التوقف وإشارات توجيه المرور وحواجز عبور البوابات تمثل جميعها نظم الرقابة الخارجية للسيارة وسائقها، وفي حين أن قائد السيارة هو المشغل لعملية - أو نظام - الرقابة الداخلية بالسيارة، إلا أن سلطة اتخاذ القرار لديه تكون ضعيفة عند التعامل مع الرسالة الموجهة إليه من إشارة ضوئية تمثل الرقابة الخارجية.

ومن منظور الرقابة الداخلية يمكن مقارنة المؤسسة بمثال السيارة الذي ذكرناه. كما سنجد عديداً من نظم وعمليات المؤسسة المفعلة مثل عمليات المحاسبة وعمليات البيع ونظم تقنية المعلومات؛ وإذا لم تقم الإدارة بتشغيل أو توجيه هذه العمليات بشكل صحيح، فإن المؤسسة ربما تعمل خارج نطاق السيطرة. ويتعين على جميع أعضاء المؤسسة بلورة فهم ما لنظم الرقابة المناسبة وتقرر من خلاله ما إذا كانت هذه النظم مرتبطة بشكل صحيح بإدارة المؤسسة. ويشار إلى هذه النظم بمسمى أنظمة الرقابة الداخلية للمؤسسة.

معلومات أساسية عن معايير الرقابة الداخلية:

على الرغم من أن مفهوم الضوابط الداخلية وتعريفها أصبح من السهل اليوم فهمها بشكل جيد فإن هذا الأمر لم يكن صحيحاً حتى أواخر ثمانينيات القرن العشرين. وعلى الرغم من أننا كنا ندرك غالباً المفهوم العام، فإنه لم يتوافق اتفاقاً ثابتاً بين العديد من المهنيين المهتمين بالأعمال والمحاسبة فيما يتعلق بالمقصود من "نظم الرقابة الداخلية

الجيدة". وتتمثل أمامنا نقطة انطلاق جيدة لذلك من خلال التعريفات الأولى التي صدرت في البداية من المعهد الأمريكي للمحاسبين القانونيين (AICPA) واستخدمتها هيئة الأوراق المالية والبورصة الأمريكية (SEC) تنفيذاً لقانون بورصة الأوراق المالية الخاص بلوائح عام ١٩٣٤. ومع حدوث تغيرات بمرور السنين، فإن معايير معهد المحاسبين القانونيين الأمريكيين (AICPA) التي تم تدوينها في البداية وكانت تسمى بيان معايير التدقيق رقم ١ (SAS No.1)^(١) حددت ممارسة التدقيق الخارجي للبيانات المالية في الولايات المتحدة لسنوات عديدة. وقد تعرض هذا التعريف الذي وضعه المعهد الأمريكي للمحاسبين القانونيين (AICPA) للرقابة الداخلية بالطبع لتغيرات وتنقيحات على مر السنين. وخلال هذه الفترة وتحديداً خلال سبعينيات القرن العشرين ظهرت تعريفات عديدة للرقابة الداخلية صدرت عن هيئة الأوراق المالية والبورصة الأمريكية (SEC) والمعهد الأمريكي للمحاسبين القانونيين (AICPA) إلى جانب العديد من التفسيرات والإرشادات التي وضعتها وطورتها بعد ذلك كبرى شركات التدقيق الخارجي.

لقد تغيرت الأوضاع في الفترة الأخيرة من سبعينيات وأوائل ثمانينيات القرن العشرين، تلك الفترة التي شهدت العديد من الإخفاقات في المؤسسات الأمريكية الكبرى نظراً لعدة عوامل منها ارتفاع معدلات التضخم وارتفاع أسعار الفائدة المصاحبة لذلك. وفي عديد من الوقائع أشارت الشركات إلى وجود أرباح مناسبة في تقاريرها المالية المدققة، في حين أنها وبعد فترة وجيزة من نشر تلك التقارير المالية المدققة الإيجابية تتعرض لانهايار مالي. لم تتسبب التقارير المالية الاحتياطية إلا في حدوث القليل من تلك الإخفاقات، في حين حدث أغلبها بسبب ارتفاع معدلات التضخم أو قضايا أخرى كانعدام الاستقرار في المؤسسات. وعلى الرغم من ذلك، فقد اقترح العديد من أعضاء الكونجرس الأمريكي سن تشريع لـ "تصحيح" الإخفاقات المحتملة في الأعمال وعمليات التدقيق، وقد تم صياغة القوانين وعقدت جلسات الاستماع في الكونجرس لكنها لم تسفر عن تمرير أي تشريع. وللقضاء على هذه المخاوف ونظراً لعدم وجود إجراء تشريعي، فقد تم تشكيل اللجنة الوطنية المعنية بدراسة وضع التقارير المالية الاحتياطية. وقد ضمت هذه اللجنة خمس منظمات مهنية هي: AICPA و IIA وقد سبق ذكرهما؛ ومعهد المديرين التنفيذيين الماليين الدوليين (FEI) وهي جمعية من كبار المديرين الماليين؛ وجمعية المحاسبين الأمريكيين (AAA)؛ ومعهد

المحاسبين الإداريين (IMA). وتعد جمعية المحاسبين الأمريكيين (AAA) منظمة مهنية تضم المحاسبين الأكاديميين، في حين يمثل معهد المحاسبين الإداريين (AMI) المنظمة المهنية للمحاسبين الإداريين أو محاسبي التكاليف.

وقد سُميت اللجنة الوطنية المعنية بوضع التقارير الاحتياطية بـ "لجنة تريدواي" نسبة إلى رئيسها، وقد اقتضت أهداف هذه اللجنة على تحديد العوامل والأسباب التي سمحت بوجود تقارير مالية احتياطية وعلى إصدار توصيات من شأنها الحد من تكرار حدوثها. وقد صدر التقرير النهائي للجنة تريدواي في عام ١٩٨٧م^(٣) وتضمن عدداً من التوصيات للعاملين في الإدارة ومجالس الإدارة وأقسام المحاسبة القانونية العمومية وغيرهم. كما دعت أيضاً إلى إعداد تقارير إدارية عن فاعلية نظم الرقابة الداخلية لديها والتأكيد على العناصر الرئيسية التي يجب توافرها في نظام الرقابة الداخلية متضمناً ذلك توافر بيئة رقابة قوية وقواعد سلوكية ولجان تدقيق معنية ومختصة وإدارة تدقيق داخلي قوية. وقد أوضح تقرير لجنة تريدواي مرة أخرى عدم وجود تعريف ثابت للرقابة الداخلية، ويشير بذلك إلى الحاجة إلى مزيد من العمل في المستقبل. وقد قامت لجنة المنظمات الراعية (COSO) نفسها التي أدارت تقرير تريدواي بالتعاقد في وقت لاحق مع مختصين من الخارج وأطلقت مشروعاً لتعريف الرقابة الداخلية، وعلى الرغم من عدم إصدار اللجنة لأية معايير، فإنها أصدرت إطاراً للرقابة الداخلية خاصاً بها ستم مناقشته في الأجزاء التالية ويشار إليه عبر فصول هذا الكتاب.

إطار الرقابة الداخلية الذي أصدرته لجنة المنظمات الراعية (COSO):

كما ذكرنا من قبل، يشير مصطلح لجنة المنظمات الراعية (COSO) إلى المنظمات المهنية الخمس العاملة في مجال التدقيق والمحاسبة، تلك المنظمات التي شكلت لجنة لوضع تقرير الرقابة الداخلية المشار إليه؛ ويحمل مسماه الرسمي "الإطار المتكامل للرقابة الداخلية"^(٣). سنشير إلى هذا الإطار عبر هذا الكتاب بعبارة "تقرير أو إطار الرقابة الداخلية" COSO، وهذا بخلاف إدارة المخاطر المؤسسية للجنة المنظمات الراعية (COSO ERM) وإطار إدارة الموارد الوارد في الفصل الثامن من هذا الكتاب. ومنذ صدور تقرير الرقابة الداخلية للجنة المنظمات الراعية (COSO) للمرة الأولى في سبتمبر ١٩٩٢ اقترح إطار مشترك لتعريف نظم الرقابة الداخلية فضلاً عن وضع إجراءات لتقييم هذه النظم الرقابية. وما إن مضت

سنوات قليلة من صدوره عام ١٩٩٢م حتى أصبح هذا الإطار هو الإرشادات المتعارف عليها في جميع أنحاء العالم لفهم ووضع رقابة داخلية فعالة في كل أنظمة الأعمال تقريباً. وتقدم الفقرات التالية وصفاً لإطار الرقابة الداخلية للجنة المنظمات الراعية (COSO) واستخدامه أداة لحوكمة تقنية المعلومات لإجراء تقديرات وتقييمات لنظم الرقابة الداخلية.

يوجد لدى جميع الشركات العامة تقريباً هيكل إجراءات رقابية معقدة، ووفقاً لشكل المخطط التنظيمي التقليدي، قد يكون هناك مستويات إدارية عليا ووسطى في وحدات التشغيل المتعددة أو ضمن الأنشطة المختلفة. وإضافة إلى ذلك، قد تختلف الإجراءات الرقابية نوعاً ما في كل من هذه المستويات والمكونات. فعلى سبيل المثال، يمكن أن تعمل إحدى وحدات التشغيل في بيئة عمل منتظمة تكون فيها العمليات الرقابية مهيكلية تماماً، في حين قد تعمل وحدة أخرى في صورة مشروع ناشئ بهيكل رسمي أقل بكثير. ومن ثم فالمستويات المختلفة للإدارة في هذه المؤسسات سيكون لها رؤى مختلفة عن كيفية التعامل مع نظم الرقابة. وإذا ما تساءلنا هنا "كيف تصف نظام الرقابة الداخلية الخاص بك؟" فإننا سنتلقى إجابات مختلفة من أشخاص من مختلف المستويات أو من وحدات كل من هذه المكونات المؤسسية.

وتقدم لنا لجنة المنظمات الراعية (COSO) وصفاً ممتازاً لهذا المفهوم متعدد الأبعاد لنظم الرقابة الداخلية، حيث وضعت تعريفاً للرقابة الداخلية كما يلي:

الرقابة الداخلية هي عملية يقوم على تنفيذها مجلس إدارة كيان معين وإدارة وغير ذلك من الأفراد ويتم تصميمها لتعطي تأكيداً معقولاً فيما يتعلق بإنجاز الأهداف في النواحي التالية:

- فاعلية وكفاءة عمليات التشغيل.
- مصداقية وضع التقارير المالية.
- الالتزام بالقوانين واللوائح المعمول بها^(٤).

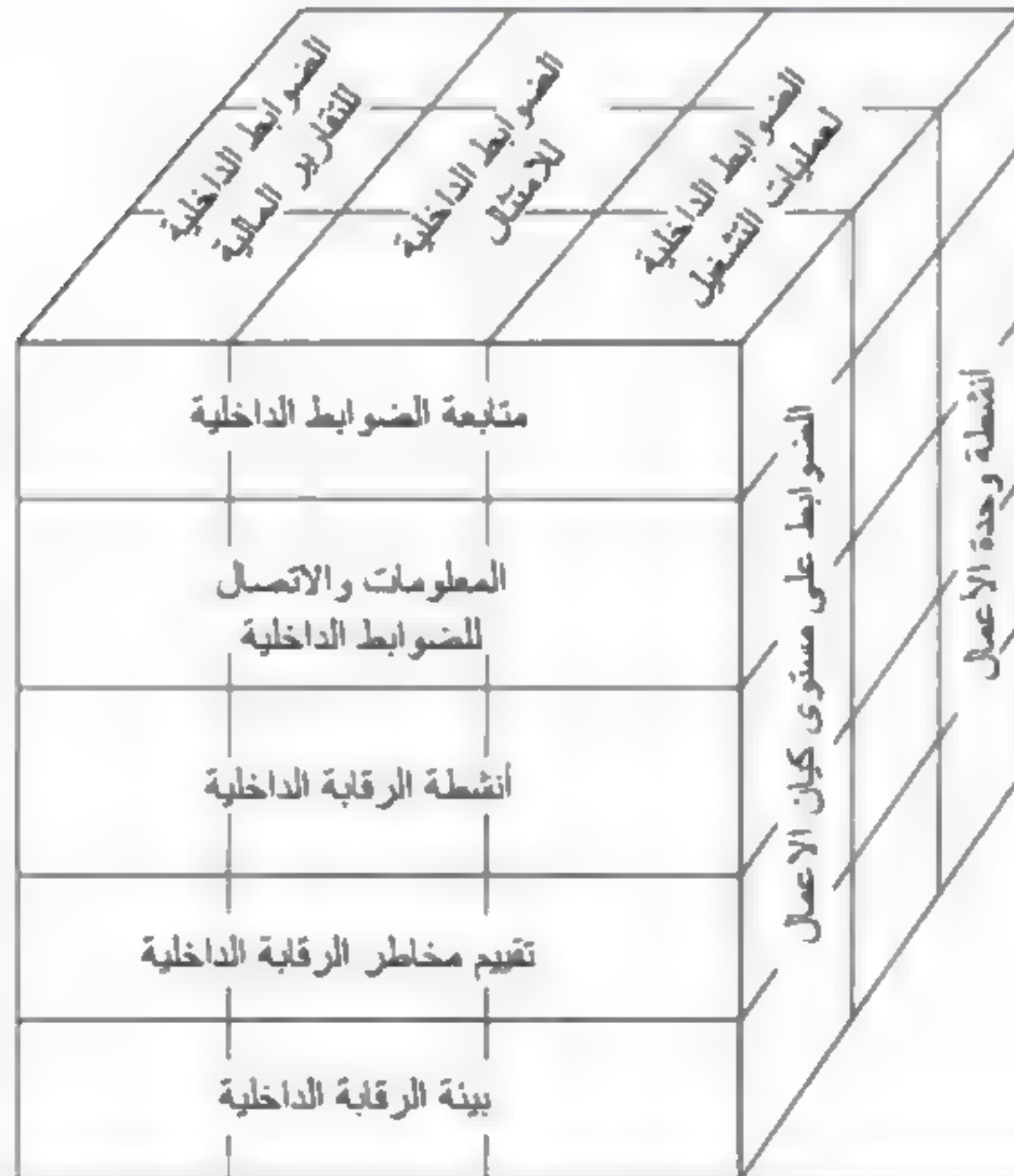
وللاستفادة من هذا التعريف الأشمل للرقابة الداخلية تستخدم لجنة المنظمات الراعية (COSO) نموذجاً أو إطاراً ثلاثي الأبعاد لوصف نظام الرقابة الداخلية في المؤسسة.

ويبين الشكل التوضيحي (١-٤) إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) على أنها نموذج ثلاثي الأبعاد بمستويات خمسة على الجانب المواجه من الشكل والمكونات الثلاثة الرئيسية للرقابة الداخلية - وهي فاعلية العمليات التشغيلية وكفاءتها وموثوقية التقارير المالية والالتزام بالقوانين واللوائح المعمول بها - تأخذ قطاعات متساوية إلى حد ما من النموذج في شكل شرائح عبر قمته، ويُبين الجانب الأيمن من الشكل ثلاثة أقسام، ومع ذلك قد يوجد عديدٌ من هذه الأقسام تبعاً لبنية المؤسسة.

كما أن كل مستوى من مستويات الجهة الأمامية من إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO)، بدءاً من المتابعة في القمة ونزولاً إلى بيئة نظم الرقابة الداخلية، سوف تتم مناقشته بمزيد من التفاصيل في الأقسام التالية.

شكل توضيحي (١-٤)

إطار الرقابة الداخلية COSO



وتدور الفكرة هنا حول أنه عندما ننظر إلى طبقة أنشطة الرقابة الداخلية في وسط النموذج - مثل الإقفال المالي في نهاية السنة المالية - فإنه يتعين علينا أن نعتبر أن الرقابة فيما يتعلق بوحدة الأعمال أو المؤسسة أو الأقسام المتعددة على جانب الإطار تعمل حيث يتم تثبيت هذا الضابط الرقابي. ومع ذلك، ففي هذا النموذج ثلاثي الأبعاد نجد أن كل ضابط رقابي مرتبط بجميع الضوابط الأخرى في الصف نفسه أو الحزمة أو العمود.

إن الهدف من إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) يتمثل في أنه ينبغي علينا دائماً أن ننظر إلى كل عنصر من عناصر الرقابة الداخلية الذي تم تعريفه طبقاً لمدى ارتباطه بعناصر الرقابة الأخرى المقترنة به في الإطار ثلاثي الأبعاد. ففي مثالنا عن نظم الرقابة الداخلية الخاصة بالإقفال المالي في نهاية السنة المالية، يتعين على المؤسسة أن تحتفظ بروابط معلومات واتصالات متعلقة بعمليات الحساب الختامي، كما يجب متابعة النظام الرقابي. وبالنزول إلى المستوى التالي، نجد ضرورة وجود أنشطة لتقييم المخاطر مصاحبة لعملية الرقابة المالية التي يجب أن تعمل في بيئة رقابة داخلية مناسبة، كما قد يكون للقضايا المتعلقة بعمليات التشغيل والامتثال عوامل مؤثرة في النظام الرقابي المتبع الذي قد يعمل على أي مستوى من الهيكل التنظيمي للمؤسسة.

وبينما تصف الأقسام التالية إطار الرقابة الداخلية للجنة المنظمات الراعية (COSO) بمزيد من التفصيل، فإنه يجب على كبار المديرين في المؤسسة فهم إطار الرقابة الداخلية للجنة المنظمات الراعية (COSO) فهماً دقيقاً وكذلك أثره في حوكمة تقنية المعلومات، وبغض النظر عن المجال قيد المراجعة يجب على كبار المديرين دائماً مراجعة نظم الرقابة الداخلية لديهم وتبنيها باعتبارها من هذا النوع متعدد المستويات وثلاثي الأبعاد. وتقوم الأقسام التالية بوصف إطار الرقابة الداخلية للجنة المنظمات الراعية (COSO) بمزيد من التفاصيل، وذلك ابتداء من أول مستوى للجهة الأمامية من الإطار أو من أسفله.

بيئة الرقابة:

يُقصد بالأساس أو المستوى السفلي من إطار الرقابة الداخلية للجنة المنظمات الراعية (COSO) ما تطلق عليه لجنة المنظمات الراعية (COSO) اسم بيئة الرقابة الداخلية.

وينبغي اعتبار بيئة الرقابة الداخلية أساساً لجميع مكونات الرقابة الداخلية الأخرى، كما أن له تأثيراً في كل من الأهداف الثلاثة وأنشطة الوحدة والمؤسسة بأكملها. كما تعكس بيئة الرقابة الداخلية التصور العام والوعي والتصرفات والأفعال من قبل مجلس الإدارة والإدارة وغيرهم بشأن أهمية نظم الرقابة الداخلية في المؤسسة. وبينما يوجد العديد من المفاهيم الأساسية هنا، فإن كل مؤسسة سيكون لديها أساس رقابة داخلية فريدٌ خاصٌ بها.

ويقوم تاريخ المؤسسة وثقافتها غالباً بالدور الرئيسي في تكوين بيئة الرقابة الداخلية هذه. فعندما يكون للمؤسسة إدارة قوية على مدار تاريخها تشدد على تقديم منتجات خالية من العيوب، وعندما تقوم الإدارة العليا بالترويج لأهمية وجود منتجات عالية الجودة إلى كل مستويات المنظمة، فإن ذلك يصبح عاملاً رئيسياً في بيئة الرقابة المؤسسية. كما أن الرسائل التي تأتي من الرئيس التنفيذي (CEO) أو من غيره من كبار مديري المؤسسة تعرف بـ "النعمة السائدة"؛ رسائل الإدارة لجميع أصحاب المصلحة. أما إذا كانت سمعة الإدارة العليا أنها "تتغاضى" عن انتهاكات سياسة المؤسسة، فإن هذا النوع نفسه من الرسائل السلبية سوف يصل بالمثل إلى المستويات الأخرى في المؤسسة. إن النعمة الإيجابية السائدة لدى الإدارة العليا تعد عنصراً أساسياً لبيئة رقابة مؤسسية قوية، سواء لعمليات تقنية المعلومات أو لجميع الأنشطة الأخرى.

ويجب على كبار المديرين أن يحاولوا دائماً إدارة بيئة الرقابة الشاملة في منظماتهم وفهمها، وتصف الفقرات التالية المكونات الأساسية لبيئة الرقابة.

النزاهة والقيم الأخلاقية:

إذا قامت المؤسسة بوضع قواعد سلوكية قوية تشدد على النزاهة والقيم الأخلاقية، وإذا ظهر التزام أصحاب المصلحة بتلك القواعد، فسيكون لدى أصحاب المصلحة جميعهم ما يكفي من الضمانات التي تفيد احتفاظ المؤسسة بمجموعة جيدة من القيم. إن مدونة القواعد الأخلاقية أو السلوكية، كما نوقشت في الفصل العشرين من هذا الكتاب، تعد مكوناً هاماً من مكونات الحوكمة المؤسسية وحوكمة تقنية المعلومات.

وعلى كل حال، حتى وإن كان لدى المؤسسة قواعد سلوكية قوية، فإن مبادئها غالباً ما قد تنتهك بسبب الجهل وليس بسبب المخالفات المتعمدة من قبل الموظف. ففي كثير من الأحيان، قد لا يدرك الموظفون أنهم يرتكبون خطأً أو قد يعتقدون خطأً أن أفعالهم تصب في مصلحة المؤسسة. هذا الجهل ينتج غالباً عن ضعف التوجيه المعنوي من قبل الإدارة العليا أكثر من كونه ناتجاً عن نية الغش من قبل الموظف، وأنه يلزم نقل سياسات المؤسسة وقيمها إلى جميع مستوياتها. وبينما قد يوجد "فاسدون" غالباً في أي مؤسسة، فإن الرسائل المعنوية القوية سوف تشجع الجميع على العمل بشكل سليم، وينبغي أن يكون الهدف دائماً نقل الرسائل أو الإشارات المناسبة إلى جميع أنحاء المؤسسة.

يتعين على أصحاب المصلحة جميعهم، وخصوصاً كبار المديرين، أن يفهموا بشكل جيد مدونة قواعد السلوك وكيفية تطبيقها. وإذا لم تعد القواعد الحالية مناسبة للزمن أو لا يبدو أنها تعالج قضايا أخلاقية هامة تواجه المؤسسة أو لا يبدو أن المؤسسة قادرة على نقل هذه القواعد إلى أصحاب المصلحة بصورة منتظمة، فإن الإدارة تكون في حاجة إلى أن "تنشط" وتصحح هذا القصور. وبينما تصف مدونة قواعد السلوك قواعد السلوك الأخلاقي، وأنه يتعين على الإدارة العليا أن تنقل الرسالة الأخلاقية السليمة في جميع أنحاء المؤسسة؛ نجد أن الحوافز والإغراءات الأخرى يمكن أن تؤدي إلى تآكل هذه البيئة الرقابية الشاملة، كما قد يميل بعض الأفراد إلى الانخراط في أعمال غير شريفة أو غير قانونية أو غير أخلاقية إذا أعطتهم مؤسساتهم حوافز أو إغراءات لعمل ذلك. على سبيل المثال، قد تقوم المؤسسة بوضع أهداف أداء غير واقعية ومرتفعة جداً للمبيعات أو حصص الإنتاج، فإذا كانت هناك مكافآت ضخمة لتحقيق أهداف الأداء تلك، أو ما هو أسوأ كوجود تهديدات قوية تنذر بفقد الأهداف؛ فإن ذلك قد يشجع الموظفين على المشاركة في الممارسات الاحتيالية أو المشكوك فيها لتحقيق تلك الأهداف.

الالتزام بالكفاءة:

يمكن أن تتآكل البيئة الرقابية للمؤسسة بشكل خطير إذا وظفت عدداً كبيراً من الأشخاص ممن يفتقدون المهارات الوظيفية المطلوبة. وهنا تظهر حاجة المؤسسة لتحديد مستويات الكفاءة المطلوبة لمهام الوظائف المتنوعة بها وكذا ترجمة هذه المتطلبات إلى مستويات

ضرورية من المعرفة والمهارة. فعند وضع الأشخاص المناسبين في الوظائف المناسبة وتدريبهم بالشكل المناسب إذا تطلب الأمر ذلك، فإن المؤسسة تكون قد حققت بذلك مكوناً مهماً للبيئة الرقابية طبقاً لإطار (COSO).

مجلس الإدارة ولجنة التدقيق:

تتأثر بيئة الرقابة بشكل كبير بأعمال مجلس إدارة المؤسسة ولجنة التدقيق فيها، فوجود مجلس إدارة فعال ومستقل يعد مكوناً أساسياً لبيئة الرقابة الخاصة بلجنة المنظمات الراعية (COSO). ومن خلال وضع سياسات رفيعة المستوى ومراجعة السلوك العام للشركة، يتحمل مجلس إدارة المؤسسة ولجنة التدقيق فيها المسؤولية المطلقة لتحديد "النغمة السائدة" داخل المؤسسة.

فلسفة الإدارة ونمط التشغيل:

إن فلسفة الإدارة العليا ونمط التشغيل الذي تعمل به له تأثير كبير في البيئة الرقابية للمؤسسة، فبعض مديري الإدارة العليا في كثير من الأحيان يتحملون مخاطر كبيرة في مشاريع أعمالهم أو منتجاتهم الجديدة، في حين يكون غيرهم حذرين جداً أو متحفزين.

ويبدو أن بعض المديرين يعملون وفق أهوائهم، في حين يصر غيرهم على ضرورة الموافقة السليمة على كل إجراء وتوثيقه كما ينبغي. كما قد يتبنى البعض نهجاً قاسياً في تفسيراتهم للقواعد الضريبية وإعداد التقارير المالية، في حين أن البعض الآخر يتبع التعليمات بدقة. ولا تعني هذه التعليمات بالضرورة أن نهجاً معيناً جيداً والآخر سيئاً على طول الخط.

إن هذه الاعتبارات الخاصة بفلسفة الإدارة والنمط التشغيلي تمثل جميعها جزءاً من بيئة الرقابة للمؤسسة. وفي حين أنه لا توجد مجموعة واحدة من الأنماط والفلسفات تكون هي الأفضل لجميع المؤسسات، فإن هذه العوامل تكون مهمة عند دراسة المكونات الأخرى للرقابة الداخلية وممارسات حوكمة تقنية المعلومات في مؤسسة ما.

الهيكل التنظيمي:

يوفر مكون الرقابة الداخلية هذا إطاراً لأنشطة التخطيط والتنفيذ والرقابة والمتابعة للمساعدة في تحقيق الأهداف العامة للمؤسسة. إن عامل بيئة الرقابة هذا يتعلق بكيفية إدارة الوحدات أو الإدارات وتنظيمها. ومع أن الهيكل التنظيمي يمثل جانباً مهماً من جوانب البيئة الرقابية للمؤسسة، فإنه لا يوجد هيكل معين يقدم لنا بيئة رقابية داخلية مفضلة.

إن الهيكل التنظيمي هو الطريقة أو النهج الموضوع لجهود العمل الفردي التي يلزم تخصيصها وتكاملها بهدف تحقيق الأهداف العامة. فكل مؤسسة تحتاج إلى خطة فعالة لتنفيذ هذا الهيكل التنظيمي، لكن ضعف نظم الرقابة في المنظمة قد يؤثر بشكل كبير في البيئة الرقابية بأكملها. وعلى الرغم من الخطوط الواضحة للسلطة، فإن المؤسسات في كثير من الأحيان تعاني بعض أوجه القصور الداخلية التي يمكن أن تزيد كلما اتسعت المؤسسات بمرور الوقت، الأمر الذي يتسبب في حدوث خلل في إجراءات الرقابة.

تخصيص السلطة والمسئولية:

يتشابه هذا الجانب من بيئة الرقابة مع مكون الهيكل التنظيمي الذي سبق مناقشته، ويحدد الهيكل التنظيمي للمؤسسة تخصيص إجمالي جهود العمل في المؤسسة وتكاملها. ويمثل تخصيص الصلاحية في الأساس الطريقة التي يتم بها تحديد المسؤوليات من حيث التوصيف الوظيفي ويتم صياغتها طبقاً لمخططات المؤسسة. وعلى الرغم من أن المهام الوظيفية لا يمكن أن تخلو تماماً من بعض المسؤوليات المتداخلة، فإنه كلما كان بيان هذه المسؤوليات أكثر دقة كان ذلك أفضل. إن الإخفاق في وضع تعريف واضح لصلاحية ومسئولية محل العمل يتسبب غالباً في الالتباس والتعارض بين جهود العمل الفردية والجماعية.

سياسات وممارسات الموارد البشرية:

تشمل ممارسات الموارد البشرية توظيف وتوجيه وتدريب وتقييم العاملين وكذلك تقديم المشورة لهم وترقيتهم ومكافأتهم واتخاذ الإجراءات الإصلاحية المناسبة بشأنهم. وبينما يتعين على إدارة الموارد البشرية الاحتفاظ بسياسات معلنة ومواد إرشادية ملائمة وكافية، فإن ممارساتها الفعلية تبعث برسائل قوية للموظفين عن المستويات المتوقعة لتوافق

الرقابة الداخلية والسلوك الأخلاقي والاختصاص. إن الموظف الأعلى الذي يتجاهل أو ينتهك صراحةً سياسة إدارة الموارد البشرية سرعان ما يبعث رسالة بما ارتكب إلى المستويات الأخرى في المؤسسة، ويزداد صدى هذه الرسالة بشكل أكبر خصوصاً عندما ينال موظف أدنى عقوبة تأديبية لانتهاكه السياسة نفسها في حين يغض الجميع الطرف عن المخالف الأعلى.

تعد سياسات إدارة الموارد البشرية وإجراءاتها الفعالة مكوناً بالغ الأهمية في بيئة الرقابة الخاصة بلجنة المنظمات الراعية (COSO) بكاملها. ولن تحقق الرسائل الواردة من قمة الهيكل القوي للمؤسسة إلا القليل إذا انعدم لدى المؤسسة إجراءات وسياسات قوية لإدارة الموارد البشرية.

خلاصة القول: كما أن الأساس المتين أمرٌ ضروري لإنشاء مبنى متعدد الطوابق، فإن بيئة الرقابة تعد أساس المكونات الأخرى للرقابة الداخلية. إن المؤسسة التي تريد أن تنشئ بنية رقابة داخلية قوية ينبغي عليها أن تولي اهتماماً خاصاً لوضع حجر أساس صلب في أساس بيئة الرقابة تلك. إن بيئة الرقابة الداخلية الخاصة بلجنة المنظمات الراعية (COSO) لا تتطلب مجرد مجموعة قواعد من نوعية "هل يتساوى الدائنون مع المدينون" لكنها تحتاج إلى سياسات قوية وفعالة وشاملة على مستوى المؤسسة.

تقييم المخاطر:

إن المستوى التالي - أو الطبقة التي تعلو مستوى بيئة الرقابة في إطار الرقابة الداخلية بلجنة المنظمات الراعية (COSO) - يمثل مستوى تقييم المخاطر. إن قدرة المؤسسة على تحقيق أهدافها يمكن أن تكون عرضة للمخاطر بسبب وجود نوعية من العوامل الداخلية والخارجية. كما أن فهم بيئة المخاطر وإدارتها يمثل عنصراً أساسياً في تأسيس الرقابة الداخلية ويجب أن تباشر المؤسسة إجراءات تُقيّم من خلالها المخاطر المحتملة التي قد تؤثر في تحقيق أهدافها المتنوعة. ويركز مكون تقييم المخاطر هذا على الرقابة الداخلية داخل المؤسسة، ويكون تركيزه أضيق بكثير من تركيز إطار إدارة مخاطر المؤسسة (COSO ERM) وقضايا إدارة مخاطر حوكمة تقنية المعلومات التي تتم مناقشتها في الفصل الثامن من هذا الكتاب.

وينبغي أن يكون تقييم مخاطر الرقابة الداخلية للجنة المنظمات الراعية (COSO) عملية استشرافية يتم تنفيذها على جميع المستويات وبشكل فعلي على جميع الأنشطة داخل المؤسسة. ويصف إطار الرقابة الداخلية للجنة المنظمات الراعية (COSO) تقييم المخاطر على أنها عملية من ثلاث خطوات:

١- تقدير تأثير المخاطرة.

٢- تقييم احتمال أو تكرار حدوث المخاطرة.

٣- البحث في كيفية إدارة المخاطرة كما ينبغي وتقييم الإجراءات التي يجب اتخاذها.

إن عملية تقييم المخاطرة الخاص بلجنة المنظمات الراعية (COSO) تُلقي بالمسئولية على الإدارة لتقييم ما إذا كانت المخاطرة مؤثرة، فإن كان الأمر كذلك، فعلى الإدارة اتخاذ الإجراءات المناسبة.

كما تؤكد الرقابة الداخلية الخاصة بلجنة المنظمات الراعية (COSO) أن تحليل المخاطر ليس عملية نظرية، ولكنه في كثير من الأحيان قد يكون حاسماً في تحقيق النجاح الشامل للكيان المؤسسي. ويجب على الإدارة، بوصفها جزءاً من التقييم الشامل الذي تجريه على الرقابة الداخلية، أن تتخذ الخطوات اللازمة لتقييم المخاطر التي قد تؤثر في المؤسسة كلها فضلاً عن المخاطر التي تدور حول مختلف أنشطة المؤسسة وكياناتها. وتوجد نوعية من المخاطر، تنتج عن عوامل داخلية أو خارجية، قد تؤثر في المؤسسة بشكل عام.

إن عنصر تقييم المخاطر الخاص بلجنة المنظمات الراعية (COSO) هو المجال الذي يدور حوله الكثير من اللغط والبلبله بسبب تشابه مسماه مع إطار إدارة المخاطر الخاص بلجنة المنظمات الراعية (COSO ERM) الذي تتم مناقشته في الفصل الثامن من هذا الكتاب. إن مكون تقييم المخاطر لإطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) يشتمل على تقييمات للمخاطر داخل مؤسسة فردية، في حين يشمل إطار إدارة المخاطر الخاص بلجنة المنظمات الراعية (COSO ERM) الكيان المؤسسي بأكمله وخارجه. وفي واقع الأمر، هاتان قضيتان منفصلتان؛ وأحدهما لا يصح أن يكون بديلاً عن الآخر.

أنشطة الرقابة:

تسمى الطبقة التالية من إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) أنشطة الرقابة وتمثل العمليات والإجراءات التي تساعد على ضمان تنفيذ الأعمال المخصصة لمعالجة المخاطر. وتوجد أنشطة الرقابة على جميع المستويات، وفي كثير من الحالات قد يتداخل بعضها مع بعض. وهي عناصر ضرورية لبناء ثم ترسيخ نظم رقابة داخلية فعالة في المؤسسة.

يحدد إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) سلسلة من هذه الأنشطة التي يمكن تصنيفها بشكل عام دليلاً إرشادياً أو تقنية معلومات أو نظم رقابة إدارية، كما يمكن توصيفها من منظور كونها أنشطة وقائية أو تصحيحية أو كاشفة. وعلى الرغم من عدم وجود مجموعة تعريفات للرقابة الداخلية تكون صالحة لجميع الأحوال، فإن نظم الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) توصي بأنشطة الرقابة التالية للمؤسسة:

- مراجعات المستوى الأعلى:

يتعين على الإدارة العليا مراجعة نتائج أدائها ومقارنة تلك النتائج بالميزانيات والإحصاءات التنافسية وغيرها من مقاييس المقارنة المرجعية. ومما يمثل هنا أنشطة رقابية تلك الإجراءات التي تتخذها الإدارة لمتابعة نتائج مراجعات المستوى الأعلى ولاتخاذ إجراءات تصحيحية.

الإدارة الفنية أو الوظيفية المباشرة:

يجب على المديرين على مختلف مستوياتهم مراجعة التقارير التشغيلية الصادرة من أنظمتهم الرقابية واتخاذ الإجراءات التصحيحية بالشكل المناسب. ويوجد لدى العديد من أنظمة الإدارة تقارير استثنائية تغطي تلك الأنشطة الرقابية. فعلى سبيل المثال، ضرورة وجود آلية في نظام أمن تقنية المعلومات للإبلاغ عن محاولات الوصول غير المصرح به، وضرورة أن يصاحب ذلك نشاط رقابي يقوم بمتابعة هذه الأحداث المبلغ عنها واتخاذ الإجراءات التصحيحية المناسبة. ويرتبط بعض هذه الأنشطة ارتباطاً وثيقاً بأفضل ممارسات مكتبة البنية التحتية لتقنية المعلومات التي تتم مناقشتها في الفصل السادس من هذا الكتاب.

معالجة المعلومات:

تحتوي نظم تقنية المعلومات غالباً على نظم رقابة للتحقق من التوافق في مجالات معينة ثم الإبلاغ عن أي استثناءات في الرقابة الداخلية. وينبغي أن تُقابل هذه البنود الاستثنائية بإجراء تصحيحي من خلال إجراءات مؤتمتة للنظم أو موظفي التشغيل أو الإدارة. وتشمل أنشطة الرقابة الأخرى نظم رقابة على تطوير نظم جديدة أو على الوصول إلى ملفات البيانات والبرامج.

نظم الرقابة المادية:

من الضروري احتفاظ المؤسسة بنظم رقابة مناسبة على أصولها المادية متضمناً ذلك التجهيزات والمخزون والأوراق المالية القابلة للتداول. ويمثل هنا البرنامج الفعال للجرد المادي الدوري نشاطاً رئيسياً من أنشطة الرقابة، كما أن تقنية المعلومات والتدقيق الداخلي يمكن أن يلعبا دوراً كبيراً في متابعة مدى الامتثال.

مؤشرات الأداء:

ينبغي على الإدارة ربط مجموعات البيانات التشغيلية والمالية بعضها ببعض واتخاذ الإجراءات التحليلية أو الاستقصائية أو التصحيحية المناسبة. وتمثل هذه العملية نشاطاً رقابياً هاماً للمؤسسة يمكن أن يلبي أيضاً متطلبات إعداد التقارير المالية والتشغيلية.

الفصل بين المهام:

يجب تقسيم المهام أو فصلها بين مختلف الأفراد للحد من مخاطر حدوث خطأ أو إجراءات غير لائقة. ويعد هذا إجراءً رقابياً داخلياً أساسياً يلزم وجوده تقريباً على شاشة رادار كل مدير أعلى.

ولا تمثل هذه الأنشطة الرقابية سوى عدد قليل من الأنشطة الكثيرة التي يتم مباشرتها ضمن السياق المعتاد للعمليات التشغيلية للأعمال، لكنها تتضمن السياسات التي تؤسس لما يجب القيام به والإجراءات اللازمة لتنفيذها. وعلى الرغم من أن أنشطة الرقابة قد يتم الإبلاغ بها شفويًا في بعض الأحيان، فإنه ينبغي تنفيذها بشكل مدروس وبأمانة واستمرارية،

وهذه رسالة قوية لمراجعة أنشطة الرقابة الداخلية تلك. وبالرغم من أن المؤسسة قد تكون صاحبة سياسة معلنة تغطي مجالاً معيناً، فإنه ينبغي أن يكون هناك إجراءات رقابة داخلية ثابتة لدعم هذه السياسة. وقد تكون هذه الإجراءات قليلة القيمة ما لم يكن هناك تركيز حاد على الحالة التي تُوجه إليها هذه السياسة. وفي أغلب الأحيان قد تنشئ المؤسسة تقريراً استثنائياً كجزء من نظام آلي يتلقى من خلاله المستفيدون أكثر من مجرد المراجعة السطحية بقليل. إلا أنه، وفقاً لأنواع الحالات المبلغ عنها، يجب أن تتلقى تلك الاستثناءات المبلغ عنها إجراءات متابعة ملائمة قد تتنوع تبعاً لحجم المؤسسة والنشاط الوارد في التقرير الاستثنائي.

ويجب أن تكون هذه الأنشطة الرقابية مرتبطة ارتباطاً وثيقاً بعضها ببعض بهدف تحديد المخاطر حسب عنصر تقييم المخاطر لإطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO). كما يجب على كبار المديرين دائماً أن يتذكروا أن الرقابة الداخلية ما هي إلا مجرد عملية وأن أنشطة الرقابة الملائمة يجب أن تُعتمد لمعالجة المخاطر المحددة. ولا يلزم اعتماد أنشطة الرقابة فقط لأنها تبدو "الشيء الصحيح الذي ينبغي عمله"، حتى إذا لم تكن هناك مخاطر كبيرة في المنطقة التي يتم فيها اعتماد النشاط الرقابي. وفي بعض الأحيان، قد تُعتمد أنشطة رقابية تكون ربما عالجت ذات مرة بعض مخاوف مخاطر الرقابة، على الرغم من أن هذه المخاوف قد تلاشت إلى حد كبير. ولا ينبغي تجاهل نشاط الرقابة لمجرد عدم وقوع أي مخالفة رقابية سابقة، لكن الرقابة تحتاج وبشكل دوري إلى إعادة تقييم للمخاطر النسبية المرتبطة بها. وينبغي أن تسهم جميع أنشطة الرقابة الداخلية في الهيكل الرقابي بشكل عام. كما يجب على مدققي تقنية المعلومات أن يضعوا هذا المفهوم في الاعتبار عند قيامهم بمراجعة الرقابة الداخلية وتقديم التوصيات. ويؤكد إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) على أن إجراءات الرقابة ضرورية لجميع نظم تقنية المعلومات الهامة: المالية والتشغيلية والمرتبطة بالامتثال. وتُقسّم نظم الرقابة الداخلية (COSO) ضوابط نظم المعلومات إلى ضوابط عامة وضوابط تطبيقات معترف بها. وتنطبق الضوابط العامة على الكثير من إدارات نظم المعلومات للمساعدة في التأكد من توافر إجراءات رقابية كافية على جميع التطبيقات. فقفّل الأمان المادي المثبت على باب مركز خوادم تقنية المعلومات يُعتبر مثلاً على الرقابة العامة لجميع

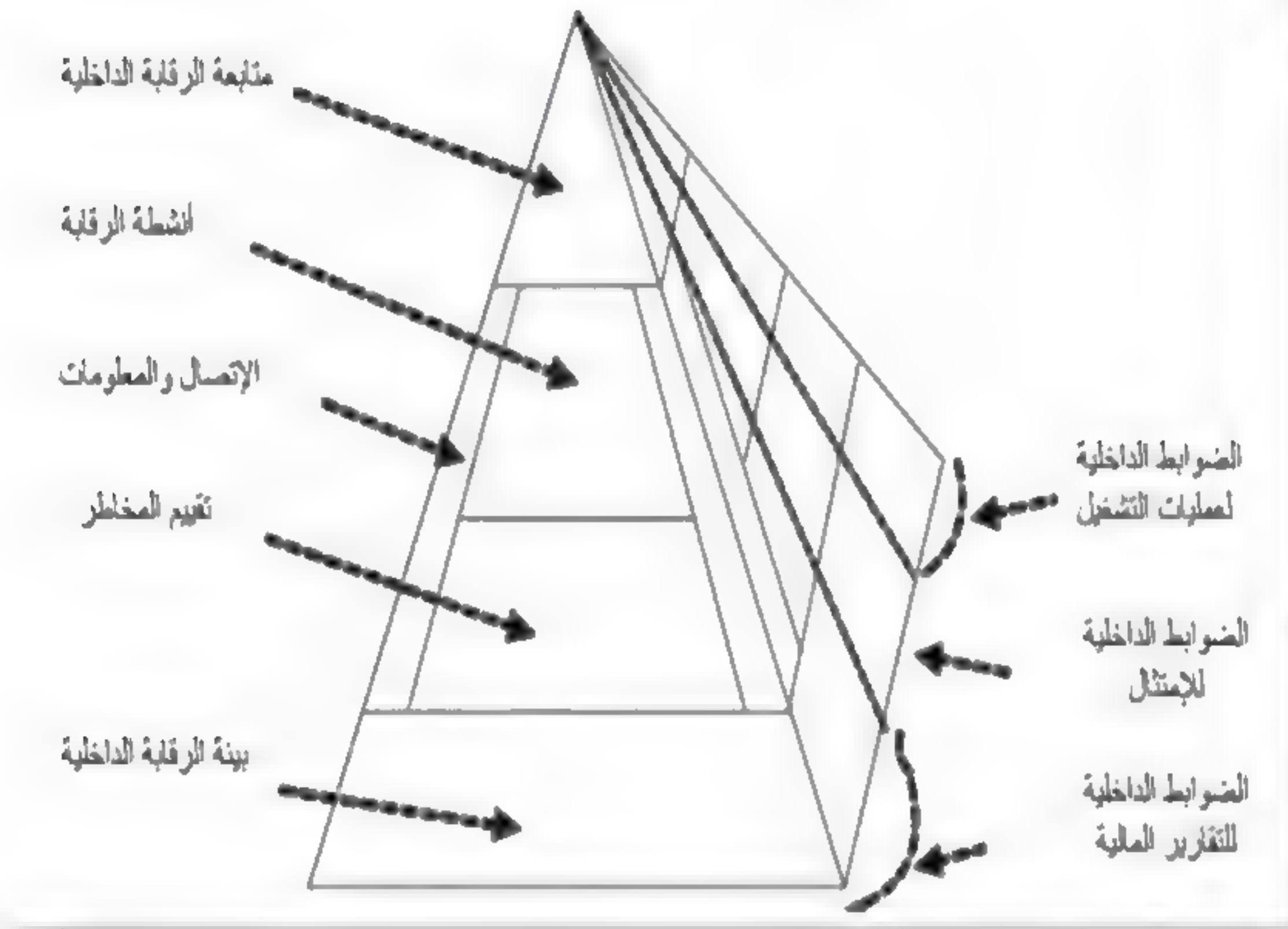
التطبيقات التي تعمل داخل المرفق. وتتم مناقشة الضوابط العامة على تقنية المعلومات في الفصل السادس. كما أن ضوابط التطبيقات التي تتم مناقشتها في الفصل العاشر من هذا الكتاب تمثل أيضاً مجالات رقابة مهمة على تقنية المعلومات لتقييم مدى كفاية نظم الرقابة الداخلية بأكملها. وتُختتم وثيقة إطار الرقابة الداخلية (COSO) بإجراء مناقشة حول ضرورة النظر في تأثير التقنيات المتطورة التي يجب أخذ تأثيرها في الحسبان دائماً عند تقييم أنشطة رقابة تقنية المعلومات. ونظراً لسرعة إدخال تقنيات جديدة فما هو جديد اليوم سرعان ما يحل محله شيء آخر.

الاتصالات والمعلومات:

يصف إطار الرقابة الداخلية (COSO) في الشكل التوضيحي (٤-١) معظم المكونات في شكل طبقات، واحدة فوق الأخرى، بدءاً من بيئة الرقابة باعتبارها الأساس. وهناك طريقة أخرى يُنظر من خلالها للإطار وهي أن تتصور إطار الرقابة الداخلية (COSO) على أنها نموذج هرمي لا تمثل فيه مكونات المعلومات والاتصالات طبقة أفقية، بل عنصراً جانبياً يمتد عبر المكونات الأخرى. وترتبط الاتصالات والمعلومات بعضها ببعض نظراً لكونها أجزاء مهمة في إطار الرقابة الداخلية، إلا أنهما يمثلان في ذات الوقت مكونات رقابية داخلية يتميز بعضها عن بعض. كما يجب نقل المعلومات المدعومة من نظم تقنية المعلومات إلى أعلى المؤسسة وأسفلها بأسلوب وإطار زمني يسمح للأشخاص بتنفيذ المهام الموكلة إليهم. وبالإضافة إلى أنظمة الاتصالات الرسمية وغير الرسمية، يجب أن يكون لدى المؤسسات إجراءات فعالة تعمل على تنفيذها للتواصل مع الأطراف الداخلية والخارجية. وكجزء من أي تقييم للرقابة الداخلية يلزم فهم تدفقات المعلومات والاتصالات والعمليات المرتبطة بها داخل المؤسسة. (انظر الشكل التوضيحي ٤-٢).

شكل توضيحي (٢-٤)

المكونات الأساسية لإطار الرقابة الداخلية COSO



وتحتاج المؤسسة إلى معلومات على جميع المستويات لتحقيق أهدافها التشغيلية والمالية والأهداف المرتبطة بمدى الامتثال. فعلى سبيل المثال، تحتاج المؤسسة إلى معلومات لإعداد التقارير المالية لتقديمها للمستثمرين الخارجيين، فضلاً عن التكلفة الداخلية ومعلومات عن تفضيلات السوق الخارجية لاتخاذ قرارات تسويقية صحيحة. ويلزم أن تتدفق هذه المعلومات من المستويات العليا للمؤسسة إلى المستويات الدنيا وكذلك من المستويات الدنيا إلى المستويات العليا عائدة. وتتخذ الرقابة الداخلية (COSO) نهجاً واسعاً لمفهوم نظام المعلومات مع الاعتراف بأن هذه الأنظمة يمكن أن تكون يدوية، آلية، أو حتى مفاهيمية. كما أن أيّاً من نظم المعلومات هذه يمكن أن تكون رسمية أو غير رسمية. كما أن المحادثات المنتظمة مع العملاء أو الموردين يمكن أن تكون مصادر معلومات مهمة جداً وتعتبر نوعاً

غير رسمي من نظم المعلومات. ويتعين على المؤسسة الفعالة أن تحتفظ بنظم معلومات تستخدمها للاستماع إلى طلبات العملاء أو الشكاوى وإحالة تلك المعلومات التي يبدونها العميل إلى الموظفين المناسبين.

كما تؤكد الرقابة الداخلية (COSO) أهمية الاحتفاظ بالمعلومات ونظم الدعم بما يتفق مع احتياجات المؤسسة بأكملها. وتتكيف نظم المعلومات لدعم التغييرات في مستويات كثيرة، فمدققو تقنية المعلومات على سبيل المثال يواجهون كثيراً حالات تكون قد شهدت تنفيذ تطبيق تقنية معلومات منذ سنوات لدعم احتياجات مختلفة. وعلى الرغم من إمكانية وجود ضوابط رقابية جيدة للنظام، فإن هذا النظام قد لا يدعم الاحتياجات الحالية للمؤسسة. وتتبنى نظم الرقابة الداخلية (COSO) رؤية شاملة لأنواع تلك النظم، كما تشير إلى الحاجة إلى فهم كل من العمليات اليدوية والتقنيات الآلية.

المتابعة:

تعرض النظرة الهرمية للرقابة الداخلية (COSO) الموضحة بالشكل التوضيحي (٤-٢) عنصر المتابعة بوصفه المستوى الأعلى والمتطور لعناصر الرقابة الداخلية (COSO). وفي حين أن نظم الرقابة الداخلية ستعمل بفاعلية مدعومة بشكل مناسب من الإدارة والإجراءات الرقابية وارتباطات المعلومات والاتصالات؛ لابد من إجراء عمليات متابعة تلك الأنشطة. كانت المتابعة ولمدة طويلة هي الدور الذي تقوم به تقنية المعلومات وغيرها من المدققين الداخليين ممن يقومون بالمراجعات لتقييم مدى الامتثال مع الإجراءات الموضوعة، لكن ومع ذلك، تتخذ نظم الرقابة الداخلية (COSO) الآن رؤية أوسع للمتابعة أيضاً، كما تعترف بأن إجراءات الرقابة وغيرها من النظم تتغير بمرور الوقت. فما ظهر أنه فعال عند بداية تثبيته قد لا يكون فعالاً في المستقبل نظراً للظروف المتغيرة والإجراءات الجديدة أو غيرها من العوامل. وقد تحتاج المنشأة إلى وضع مجموعة متنوعة من أنشطة المتابعة لقياس مدى فاعلية نظم الرقابة الداخلية لديها من خلال عمليات تقييم منفصلة إلى جانب القيام بأنشطة مستمرة لمراقبة الأداء واتخاذ إجراءات تصحيحية عند الحاجة. فالعديد من إدارات الأعمال الروتينية يمكن تصنيفها على أنها أنشطة متابعة، وتعطي (COSO) أمثلة على هذا المكون المهم من مكونات الرقابة الداخلية:

الوظائف الاعتيادية لإدارة التشغيل:

تعد المراجعات الاعتيادية التي تجريها الإدارة لعمليات التشغيل والتقارير المالية أحد أنشطة المتابعة المستمرة الهامة، ولكن ينبغي أن نُولي اهتماماً خاصاً بالاستثناءات المرصودة وانحرافات الرقابة الداخلية، ومما يعزز الرقابة الداخلية مراجعة التقارير بصفة منتظمة واتخاذ إجراءات تصحيحية لأي استثناءات مرصودة.

اتصالات من أطراف خارجية:

تعتبر وسائل مراقبة الاتصالات الخارجية مثل رقم هاتف شكاوى العملاء من الأمور المهمة. كما تحتاج المؤسسة أن تتابع تلك المكالمات عن كثب وتنفذ الإجراءات التصحيحية بناء على هذه المكالمات كلما دعت الحاجة لذلك.

البنية المؤسسية والأنشطة الرقابية:

على الإدارة العليا دائماً القيام بمراجعة تقارير موجزة واتخاذ إجراءات تصحيحية بشأنها، ويلعب والمستوى الرقابي الأول في الغالب دوراً أكثر أهمية في عملية المتابعة. كما أن الرقابة المباشرة للأنشطة الكتابية، على سبيل المثال، ينبغي أن تراجع بشكل روتيني أخطاء المستوى الأدنى وتُصحح، كما يتعين عليها أن تضمن تحسين أداء الموظفين الكتبة. ويمثل هذا أيضاً أحد المجالات التي يكون من الأهمية بمكان القيام بفصل كاف بين المهام، كما أن تقسيم المهام بين الموظفين يسمح لهم بالقيام بدور متابعة بعضهم لبعض.

الجرد المادي وتسوية الأصول:

إن عمليات الجرد المادي الدوري، سواء لمخزون المستودعات أم الأوراق المالية القابلة للتداول أو أصول تقنية المعلومات، تعد من بين أنشطة المتابعة المهمة. فالجرد السنوي في متجر بيع تجزئة مثلاً قد يشير إلى فقد كبير في البضاعة، وقد يكون أحد الأسباب المحتملة لهذا الفقد هو شبهة سرقة، مما يشير إلى ضرورة وجود نظم رقابة أمنية أفضل.

وليست هذه سوى أمثلة قليلة من أنشطة المتابعة لنظم الرقابة الداخلية (COSO) التي تُعتبر أشكالاً من الإجراءات التي ينبغي تنفيذها في العديد من المؤسسات، لكنها في كثير من

الأحيان لا يُنظر إليها على أنها أنشطة متابعة مستمرة. فأي إدارة أو عملية تقوم بمراجعة أنشطة المؤسسة بصفة مستمرة، ثم تقترح إجراءات تصحيحية محتملة يجب النظر إليها باعتبارها نشاط متابعة. وفي حين يشير إطار الرقابة الداخلية (COSO) إلى أهمية أنشطة المتابعة هذه، فإنه يشير أيضاً إلى أنه "قد يكون من المفيد إلقاء نظرة جديدة من وقت لآخر على فاعلية نظم الرقابة الداخلية من خلال القيام بتقييمات منفصلة". وتعتمد وتيرة تلك التقييمات أو المراجعات المنفصلة وطبيعتها بشكل كبير على طبيعة المؤسسة وأهمية المخاطر التي يجب مراقبتها.

وحين ترغب الإدارة في بدء إجراء تقييم دوري لنظم الرقابة الداخلية لديها بكاملها، ففي الغالب يجب أن تبدأ بتقييم مجالات رقابية محددة. ويبدأ إجراء هذه المراجعات غالباً عندما تكون هناك عملية استحواذ أو تغيير في قطاع العمل أو في بعض الأنشطة المهمة الأخرى.

وتؤكد (COSO) أيضاً أنه يمكن إجراء هذه التقييمات من قبل الإدارة التنفيذية المباشرة من خلال إجراء مراجعات تقييم ذاتي. ومع ذلك، يجب على الإدارة المسؤولية في هذا المجال أن تتابع جدولاً هذه التقييمات الذاتية وإجراءها بصفة مستمرة. إن هذا النوع من المراجعة المتولدة داخلياً يمكن أن يشير إلى مشاكل رقابية محتملة ويتسبب في أن تقوم إدارة التشغيل بتنفيذ الأنشطة المتعلقة بالإجراءات التصحيحية. ولأن مراجعات التقييم الذاتي تلك لن تكون شاملة مثل التدقيق الداخلي النمطي، فيجب البدء في مراجعات المتابعة إذا تصادف وجود مشاكل كبيرة محتملة، وذلك من خلال القيام بمراجعات تقييم ذاتي محدودة.

عملية تقييم الرقابة الداخلية:

تلخص المواد الإرشادية للرقابة الداخلية (COSO) عملية تقييم مراجعة نظم الرقابة الداخلية. فينبغي لمثل هذا المُقيِّم أولاً أن ينمي لديه فهم تصميم النظام، ثم يقوم باختبار نظم الرقابة الأساسية، ثم يضع استنتاجات بناءً على نتائج الاختبار. كما تشير نظم الرقابة الداخلية (COSO) إلى المقارنة المرجعية، على أنها نهج بديل. وتُعرف المقارنة المرجعية بأنها عملية مقارنة عمليات المؤسسة وإجراءات الرقابة لديها مع مثيلاتها في نظائرها من المؤسسات الأخرى. فيتم إجراء المقارنات مع مؤسسات مماثلة أو مع ما يقابلها من إحصاءات الصناعة المنشورة. ويكون هذا النهج مناسباً لبعض الإجراءات وممتهلاً بالمخاطر

للبعض الآخر. فمثلاً يكون من السهل نسبياً أن تقيس حجم التوظيف ومستوياته ومتوسط التعويضات لوظيفة المبيعات مع ما يقابلها من المؤسسات المماثلة في الصناعة العامة نفسها. ومع ذلك، فإن المُقيّم قد يواجه صعوبات في محاولته مقارنة عوامل أخرى بسبب العديد من الاختلافات الصغيرة التي تجعل جميع المؤسسات فريدة من نوعها.

خطط عمل التقييم:

تقر نظم الرقابة الداخلية (COSO) بأن العديد من الإجراءات الفعالة للغاية تكون غير رسمية وغير موثقة. كما أن العديد من نظم الرقابة غير الموثقة هذه يمكن اختبارها وتقييمها بالأسلوب نفسه المتبع في اختبار النظم الموثقة وتقييمها. وحيث إن وجود مستوى مناسب من التوثيق يجعل أي تقييم لنظم الرقابة الداخلية أكثر كفاءة ويسهل فهم الموظفين لكيفية إجراء العمليات، فإن هذا التوثيق لا يكون ضرورياً بصورة مستمرة. فأي مراجعة لأنظمة الرقابة المالية الداخلية في المؤسسة سيبحث بالتأكيد عن مستوى معين من توثيق النظم كجزء من أعمال المراجعة. فإذا وجدت عملية حالية غير رسمية وغير موثقة لكن فاعليتها محل توافق، فإن فريق المراجعة المعين سيكون بحاجة إلى إعداد توثيق إجراءات التقييم بهدف شرح كيفية تنفيذ هذه العملية وطبيعة نظم الرقابة الداخلية لديها.

الإبلاغ عن أوجه القصور في الرقابة الداخلية:

سواء تم تحديد أوجه قصور الرقابة الداخلية من خلال العمليات الموجودة في نظام الرقابة الداخلية ذاته أو من خلال أنشطة المتابعة أو الأحداث الخارجية الأخرى، فإنه يلزم تبليغها إلى المستويات المختصة في إدارة المؤسسة.

والسؤال الرئيسي الذي يطرحه أي مُقيّم نظم رقابة داخلية هو تحديد ما ينبغي الإبلاغ عنه في ضوء الكم الهائل من التفاصيل التي يمكن أن تواجهه، ولمن يجب أن توجه هذه التقارير. وتنص نظم الرقابة الداخلية (COSO) على أن، "جميع أوجه القصور في نظم الرقابة الداخلية التي يمكن أن تؤثر في تحقيق المنشأة لأهدافها يجب الإبلاغ عنها لأولئك الذين يمكنهم اتخاذ الإجراءات اللازمة". ورغم أن هذا البيان الصادر من نظم الرقابة الداخلية (COSO) يوحي بدايةً بأن الأمر معقول، فإن كبار المديرين من ذوي الخبرة

يدركون أنه يكون من الصعب تطبيقه غالباً. إن المؤسسات الحديثة، بغض النظر عن تنظيمها الجيد، ستكون مدانة بسبب ارتكابها للعديد من الأخطاء أو الإهمال في نظم الرقابة الداخلية. وتشير نظم الرقابة الداخلية (COSO) إلى أن كل هذه الأمور ينبغي تحديدها والإبلاغ عنها، حتى ما يبدو أنه أخطاءً صغيرةً يجب فحصه لفهم ما إذا كانت ناجمة عن أي قصور في الرقابة بكاملها.

وتستخدم المواد الإرشادية المنشورة من قبل نظم الرقابة الداخلية (COSO) مثال الموظف الذي استولى على بضعة دولارات من صندوق المصروفات النثرية، حيث يمكن اعتبار ذلك مسألة بسيطة نظراً لصغر المبلغ المسروق، لكن يكون من الضروري اعتباره انهياراً لنظم الرقابة على عدة مستويات.

ففي حين أن المبلغ النقدي قد لا يكون كبيراً، فإن نظم الرقابة الداخلية (COSO) تحث على أنه يجب فحص هذه المسألة بدلاً من تجاهلها، لأن "هذا التغاضي الواضح عن الاستخدام الشخصي لمال المنشأة قد يرسل رسالة غير مقصودة للموظفين". فقبل ظهور قوانين ساربينز-أوكسلي (SOX)، طبق المدققون الخارجيون بانتظام مفهوم ما كان يسمى "الأهمية النسبية" عند القيام بإجراء المراجعات وقرروا أن بعض الأخطاء والمخالفات كانت صغيرة لدرجة أنها غير جوهرية بالنسبة للاستنتاجات الكلية للمدقق الخارجي.

وفي السنوات الأولى من مراجعات امتثال قوانين ساربينز-أوكسلي (SOX) مع معايير التدقيق AS2 الأصلية، كانت رسالة العديد من المدققين الخارجيين تفيد أن الأهمية النسبية لا تؤخذ بعين الاعتبار، فالخطأ هو الخطأ، وقد تسبب هذا النهج في الشعور بالإحباط لدى العديد من المديرين الذين تعجبوا من قيام مدققيهم الخارجيين بإثارة قضايا كانوا يرونها قضايا بسيطة، أما الآن ومع قوانين ساربينز-أوكسلي (SOX) الحالية التي ناقشناها في الفصل الثاني من هذا الكتاب، فقد وُضعت الأهمية النسبية والمخاطر النسبية في الاعتبار عند تقييم كفاءة نظم الرقابة الداخلية وفعاليتها.

وتختتم الإرشادات الصادرة عن نظم الرقابة الداخلية (COSO) بالنقاش حول من ينبغي توجيه تقرير أوجه قصور نظم الرقابة الداخلية إليه في المؤسسة، وتنص الفقرة الأولى منه على توجيه يفيد في التقييمات:

"إن الآثار الناتجة عن أوجه قصور نظم الرقابة الداخلية يجب الإبلاغ عنها ليس للشخص المسئول عن الإدارة أو النشاط المعني الذي يمكنه بحكم منصبه اتخاذ الإجراءات التصحيحية فحسب، لكن يجب الإبلاغ عنها في الوقت نفسه لمستوى واحد على الأقل من مستويات الإدارة الأعلى من الشخص المسئول بشكل مباشر. فهذه العملية تمكن ذلك الفرد من تقديم الدعم اللازم أو الإشراف على اتخاذ الإجراءات التصحيحية وعلى التواصل مع الآخرين في المؤسسة الذين قد تتأثر أنشطتهم. وحيث إن هذه الآثار قد تتخطى الحدود التنظيمية، فإن الإبلاغ عنها كذلك يجب أن يُنقل إلى مستوى أعلى بالدرجة الكافية ويوجه لضمان اتخاذ الإجراءات المناسبة".

كما ينبغي على المؤسسة أيضاً أن تطور إجراءات الإبلاغ بحيث يتسنى إبلاغ المستويات المناسبة في المؤسسة بكل أوجه قصور نظم الرقابة الداخلية التي تتم مواجهتها من خلال مراجعة العمليات الجارية. ويعتبر إعداد التقارير الإدارية والمتابعة جانباً مهماً للغاية من جوانب نظم الرقابة الداخلية، كما أن للتدقيق الداخلي دوراً رائداً في هذه العملية من خلال مراجعات تدقيق تقنية المعلومات، ويجب أن نعي أيضاً الحاجة إلى عمليات متابعة أخرى عند مراجعة الرقابة الداخلية وتقييمها.

أبعاد أخرى لإطار الرقابة الداخلية (COSO):

ننسى أحياناً أن إطار الرقابة الداخلية (COSO) عبارة عن نموذج ثلاثي الأبعاد كما هو مبين بالشكل التوضيحي (٤-١)، وبالإضافة إلى البعد الخاص بالواجهة الأمامية الذي يغطي أنشطة الرقابة، فإن البعد الخاص بالجهة اليمنى يغطي الكيانات أو الأنشطة، في حين أن الجزء العلوي من مكعب الإطار يغطي جميع عناصر نظم الرقابة الداخلية:

١- فاعلية العمليات وكفاءتها.

٢- موثوقية التقارير المالية.

٣- الامتثال للقوانين واللوائح المعمول بها.

كل مجال من مجالات الرقابة الذي تم مناقشته حالياً – من بيئة الرقابة إلى المتابعة – يجب أن يؤخذ أيضاً بعين الاعتبار بالنسبة للبعدين الآخرين.

وفيما يتعلق بالبعد الخاص بالجانب الأيمن، يجب تثبيت نظم الرقابة الداخلية وتقييمها عبر جميع الوحدات في المؤسسة. ولا يعني هذا أن نشاطاً رقابياً ما كعملية اعتماد المصروفات مثلاً يجب أن يكون متطابقاً في جميع وحدات المنظمة، سواء في المقر الرئيسي للمؤسسة أم في مكتب مبيعات يقع في منطقة جغرافية نائية. ومع ذلك، يلزم وجود مجموعة متناغمة من عمليات الرقابة عبر المؤسسة بأكملها مع مراعاة الاعتبارات المخصصة للتعامل مع المخاطر النسبية ونطاقات عمليات التشغيل. كما ينبغي أن تكون نظم الرقابة الداخلية متوافقة غير أنه يتم تطبيقها بشكل مناسب في وحدات التشغيل الفردية.

وبالنسبة للبعد الثالث أو العلوي من إطار نظم الرقابة الداخلية (COSO)، فإنه يمثل أهمية أكبر، حيث يفيد بأنه يجب وضع أنشطة الرقابة الداخلية في جميع وحدات تشغيل المؤسسة مع الأخذ في الاعتبار عوامل الرقابة الداخلية الثلاثة: الفاعلية وموثوقية التقارير المالية والامتثال التنظيمي. وعند النظر إلى نظم الرقابة الداخلية من هذا المنظور الثلاثي الأبعاد، ستظهر دائماً بعض الاختلافات، لكنها ستكون تحت إطار رقابة داخلية أساسي ومتسق. فعند استخدام مثال الشركة التابعة في آسيا الوسطى بعيداً عن المقر الرئيسي في الولايات المتحدة، قد تخضع إجراءات اعتماد مصروفات الدولة للقوانين المحلية، كما أن غيرها من العمليات قد تكون مختلفة بعض الشيء نظراً لبعدها الاتصالات أو الاختلافات في نظم تقنية المعلومات المحلية. ومع ذلك، يظل من الضروري تنفيذ نظم الرقابة الداخلية تلك على نحو يضمن موثوقية إعداد التقارير المالية إلى جانب إحالة النتائج إلى المقر الرئيسي للمؤسسة.

ومن بين المفاهيم المهمة والمعتبرة للغاية التي تدعم نظم الرقابة الداخلية (COSO) أن جميع الاعتبارات الخاصة بالرقابة الداخلية يتعين النظر إليها طبقاً لمكعب (COSO) ثلاثي الأبعاد، بمعنى أن الرقابة يجب أن تؤخذ في الاعتبار من ناحية توافقها مع المؤسسة بأكملها وعلاقتها بمجالات أهداف الرقابة الثلاثة التي تمت مناقشتها حالاً. ويقدم هذا المفهوم وسيلة فعالة للنظر في نظم الرقابة الداخلية من منظور شمولي. ويظل إطار الرقابة الداخلية (COSO) يمثل معياراً مهماً ومجموعة من المواد الإرشادية لقياس الرقابة الداخلية وتقييمها.

لقد أصبح إطار الرقابة الداخلية (COSO) المعيار المعتمد في جميع أنحاء العالم لبناء رقابة داخلية فعالة وتطويرها. إنها عملية مستمرة في كل من أبعاده الثلاثة. فعنصر المتابعة الموجود أعلى الجهة الأمامية من النموذج لن تكون له قيمة تذكر ما لم تُفعل عمليات الرقابة الداخلية جميعها حتى نصل بها إلى أساس بيئة الرقابة الداخلية. وعلى نحو مماثل، يجب وضع رقابة داخلية فعالة في جميع مستويات وحدات المنظمة، ويلزم أن تراعي نظم الرقابة هذه عناصر الرقابة الداخلية الثلاثة الموجودة أعلى النموذج.

إرشادات متابعة أنظمة الرقابة الداخلية (COSO):

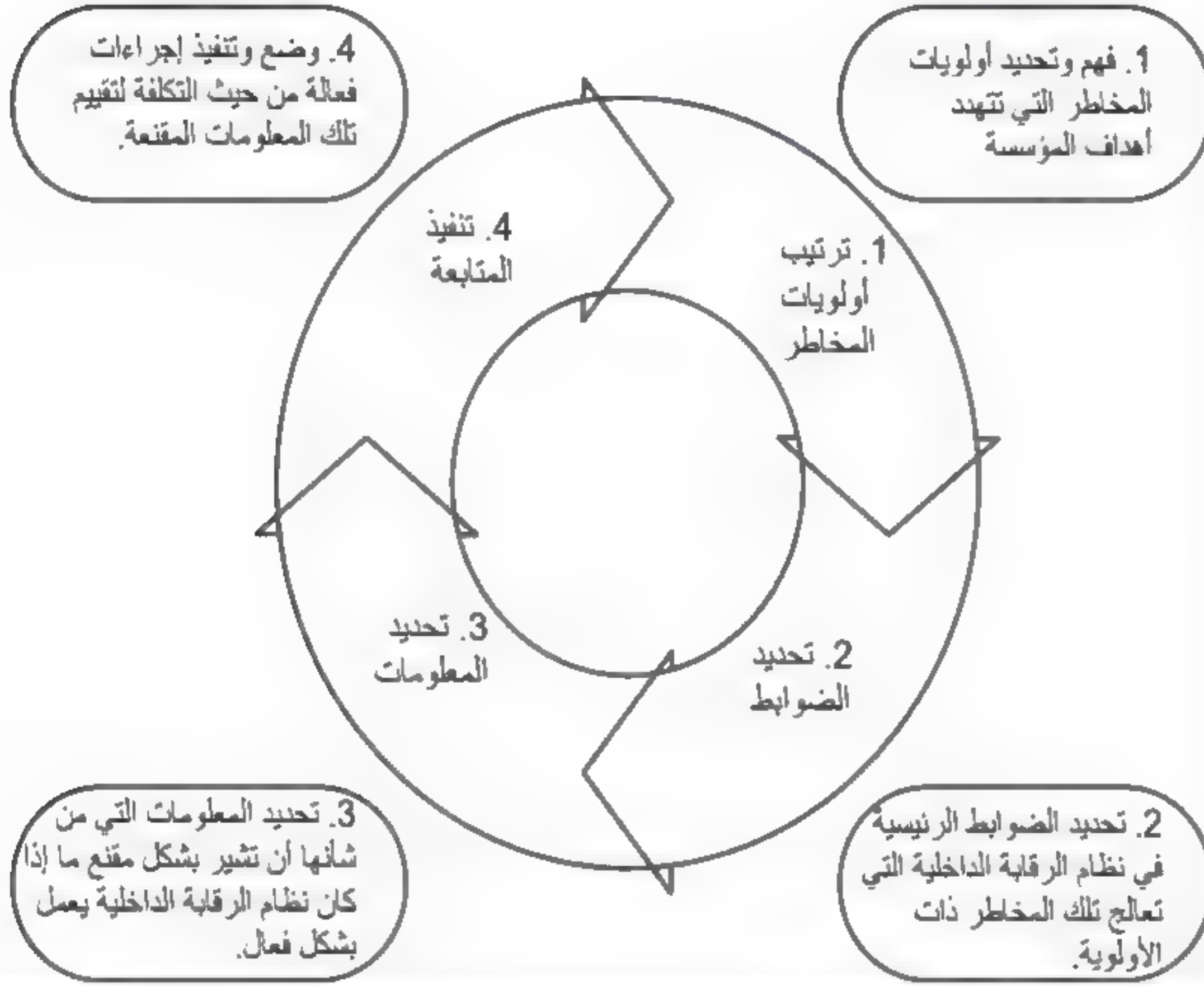
لقد أصبحت المواد الإرشادية واسعة الانتشار عن إطار الرقابة الداخلية (COSO) متاحة من خلال مصادر تتراوح بين معايير تدقيق (AICPA) إلى مختلف مواد (ISACA) بالإضافة إلى موادنا الإرشادية الإضافية^(٥)، ومع ذلك فإن العديد من المؤسسات وليس بالضرورة محترفي التدقيق قد ترغب في الحصول على إرشادات أكثر تحديداً عن كيفية تنفيذ نظم الرقابة الداخلية (COSO) في العمليات التشغيلية لأعمالها. وقد نشرت COSO مجموعة مواد إرشادية مكونة من ثلاثة مجلدات عن نظم الرقابة الداخلية في عام ٢٠٠٩م^(٦).

وتؤكد المجلدات الثلاثة لهذه المجموعة الممتازة بوجه عام أهمية متابعة فاعلية النظم الرقابية الموضوعية. وعلى الرغم من وصفنا لإطار الرقابة الداخلية (COSO) كما هو مبين بالشكل التوضيحي (٤-٢) يُظهر أن المتابعة تعد رأس العملية بكاملها، فإن هذه الدراسة الخاصة بـ COSO تشير إلى أن بعض المؤسسات لم تستغل بالشكل الأمثل نتائج أنشطة متابعتها للخروج باستنتاجات عن فاعلية عمليات الرقابة الداخلية لديها، مما أدى في بعض الأحيان إلى إجراء عمليات غير فعالة تنقصها الكفاءة.

هذه الإرشادات المتعلقة بأنظمة المتابعة الداخلية توحى بأن المؤسسات تنفذ عمليات المتابعة الخاصة بالرقابة الداخلية على غرار الطريقة التي تراقب بها المنظمات الصناعية الفاعلية والكفاءة المستمرة لإجراءات التصنيع لديها. وتقترح المواد بأن تقوم المؤسسات باعتماد عملية متابعة من أربع مراحل كما هو موضح بالشكل التوضيحي (٤-٣).

شكل توضيحي (٣-٤)

عملية متابعة تصميم وتنفيذ الإطار COSO



ينص هذا النهج ذو المراحل الأربع أنه ينبغي على المؤسسة أولاً أن تقوم بتحديد الأولويات وفهم المخاطر التي تتعرض لها أهدافها التنظيمية، ثم تحدد النظم الرقابية التي تعالج تلك المخاطر ذات الأولوية. ثم تأتي الخطوة الثالثة وهي تحديد المعلومات التي من شأنها أن تشير بشكل مقنع إلى أن نظام الرقابة الداخلية يعمل بشكل فعال. ويدعو النموذج المقترح إلى القيام بإجراءات مجدية التكلفة لتقييم المعلومات التي تم جمعها من خلال عمليات المتابعة.

تتمة: أهمية الرقابة الداخلية (COSO):

يقدم هذا الفصل إطار الرقابة الداخلية (COSO) بالغ الأهمية. فمديرو الإدارة العليا يعملون في بيئات مؤسسية متنوعة، واليوم سيواجهون في الغالب متطلبات إطار الرقابة الداخلية (COSO). وعلى الرغم من تقديم هذا الفصل لمجرد وصف موجز للرقابة الداخلية (COSO)، فإن المديرين التنفيذيين سيواجهون هذه القضايا عندما يقوم المدققون الخارجيون لديهم بمراجعة نظم الرقابة الداخلية باعتبار ذلك جزءاً من التدقيق المالي، وكذلك عندما يقوم مدققوهم الداخليون بمراجعة نظم الرقابة الداخلية في مجموعة متنوعة من المجالات.

كما يقدم إطار الرقابة الداخلية (COSO) أساساً لفهم مدى واسع من قضايا حوكمة تقنية المعلومات التي تناقش في فصول أخرى لاحقاً. ومن ثم فإن كبار المديرين يتعين عليهم تكوين معرفة عامة وفهم لإطار الرقابة الداخلية (COSO) أساساً لفهم نظم الرقابة الداخلية للمؤسسة وكذا المسائل المتعلقة بحوكمة تقنية المعلومات.

ملاحظات:

١. بيان معايير التدقيق رقم ١، تقنين معايير وإجراءات التدقيق، AICPA، المعايير المهنية.
٢. تقرير اللجنة الوطنية حول التقارير المالية الاحتيالية (National Commission on Fraudulent Financial Reporting, 1987).
٣. الرقابة الداخلية - إطار متكامل. هذا المرجع خاص بتقرير الضوابط الداخلية الصادرة عن COSO والذي يمكن طلبه من خلال المعهد الأمريكي للمحاسبين القانونيين AICPA على الموقع www.cpa2biz.com.
٤. تم وصف معايير الرقابة الداخلية الخاصة بلجنة المنظمات الراعية COSO في بيانات معايير التدقيق (SASs) أرقام 103، 105، 106، 107، 109، 110، 112.
٥. انظر "Robert Moeller, Sarbanes-Oxley Internal Controls: Effective Auditing" (with AS5, CobiT, and ITIL (Hoboken, NJ: John Wiley & Sons, 2008).
٦. Guidance on Monitoring Internal Control Systems (COSO, 2009).

الفصل الخامس

إطار كوبت (COBIT) ومعهد حوكمة تقنية المعلومات

يحتاج المهنيون المحترفون في المؤسسة وخصوصاً كبار المديرين أيضاً إلى استخدام مجموعة من المعايير أو أطر العمل لضبط كل من الممارسات المتعلقة بحوكمة تقنية المعلومات والإجراءات العامة الخاصة بالرقابة الداخلية. فالالتزام بإطار كهذا سيتيح فرصة اعتماد كبار المديرين وكذلك المهنيين داخل المؤسسة كل في مجال عمله بوصفهم أخصائيين في مجالات أعمالهم. وقد أصبح إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO) الذي تم عرضه ومناقشته في الفصل الرابع من هذا الكتاب من الأدوات الهامة في مجال حوكمة تقنية المعلومات والذي يُستخدم لتقييم وتحسين عمليات حوكمة تقنية المعلومات المتعلقة بالعديد من النظم والعمليات الخاصة بتقنية المعلومات، ويستخدم أيضاً لتقييم وتحسين قواعد الرقابة المحاسبية الداخلية وفقاً لقانون ساربينز - أوكسلي (SOX)، الذي تطرقنا إليه في الفصل الثاني من هذا الكتاب. وعلى الرغم من ذلك، فقد أعرب بعض كبار المديرين والمهنيين ممن يعملون معهم في مجال تقنية المعلومات على وجه الخصوص عن مخاوفهم من استخدام إطار الرقابة الداخلية (COSO) في ظل عالمنا اليوم المتجه نحو تقنية المعلومات. وقد جاء هذا القلق بسبب عدم تركيز الإرشادات المنشورة والخاصة بإطار الرقابة الداخلية (COSO) على أدوات وعمليات تقنية المعلومات بشكل كافٍ. فعلى سبيل المثال، تطرقت المواد الإرشادية الأصلية الخاصة بإطار الرقابة الداخلية (COSO) والتي تم نشرها عام ١٩٩٢م (انظر الفصل الرابع) في الأساس إلى الضوابط الداخلية الخاصة بتطبيقات تقنية المعلومات على مستوى عالٍ، مع أن هناك حاجة لمزيد من الإرشادات المتعلقة بالرقابة الداخلية لتقنية المعلومات في الوقت الراهن.

إن الإطار الأكثر توجهاً نحو تقييم الرقابة الداخلية لتقنية المعلومات والإرشادات المتعلقة بها يطلق عليه اسم إطار كوبت Control Objectives for Information and related Technology COBIT (أهداف ضوابط المعلومات والتقنيات ذات الصلة)، وهو الإطار المعمول به في الواقع قبل سن قانون ساربينز أوكسلي (SOX) بوقت طويل، وذلك من خلال

الإصدار الأول له عام ١٩٩٦. وقد تم تطوير الإطار كوبت بداية لدعم المدققين الداخليين والخارجيين الذين يقومون بعمليات مراجعة النظم الحاسوبية والضوابط التقنية (يطلق عليهم غالباً اسم مدققي تقنية المعلومات IT auditors). لكن كوبت أصبح هذه الأيام هو الأداة المفضلة بالنسبة للعديد من المؤسسات لتحقيق الإمتثال للبند ٤٠٤ من قانون SOx الذي يتحدث عن إجراءات الرقابة الداخلية ودعم حوكمة تقنية المعلومات المتعلقة بها. فالإطار كوبت يقدم الإرشادات اللازمة لتقييم وفهم الضوابط الداخلية لتقنية المعلومات المؤسسية ويركز على موارد تقنية المعلومات لدى المؤسسة. لا يمكن اعتبار الإطار كوبت بديلاً عن إطار الرقابة الداخلية COSO، غير أنه عبارة عن طريقة مختلفة ومفضلة في بعض الأحيان للقيام باختبار ضوابط الرقابة الداخلية في ظل عالمنا اليوم المتمركز حول تقنية المعلومات.

وعلى الرغم من إطلاق "كوبت" بالأساس ليعمل كدليل توجيهي يساعد مدققي تقنية المعلومات الداخليين والخارجيين الذين يقومون بمراجعة الضوابط الداخلية المتعلقة بتقنية المعلومات، فإنه تطور هذه الأيام ليصبح بمثابة الأداة المساعدة لتقييم حوكمة تقنية المعلومات وجميع الضوابط الداخلية في المؤسسة. فهو يؤكد الروابط الموجودة بين موارد تقنية المعلومات والموارد الأخرى للأعمال ويوفر الإرشادات الداعمة لهذه الروابط وذلك لتقديم القيم الكاملة للمؤسسة، كما يعد هذا الإطار واحداً من الأدوات الهامة لمساعدة السلطة التنفيذية العليا في المؤسسة على إيجاد ممارسات فعالة لحوكمة تقنية المعلومات.

سيقدم هذا الفصل نظرة عامة على المستوى التنفيذي للإطار كوبت والعديد من مكوناته الأساسية. وسيستعرض أيضاً الإصدار الخامس والأخير لهذا الإطار حتى وقت نشر هذا الكتاب. كما سيقوم بتقديم عناصر أخرى للإطار كوبت مثل الإرشادات الخاصة بحوكمة مجلس الإدارة والإطار الخاص بقيمة تقنية المعلومات (Val-IT) المرتبط بالإطار كوبت، وهو نهج يستخدم للتعرف على القيمة الخاصة بجميع أصول تقنية المعلومات في المؤسسة بشكل أفضل. حيث يتناول إطار قيمة تقنية المعلومات Val-IT الافتراضات والتكاليف والمخاطر والنتائج المتعلقة بالمحافظة المتوازنة لاستثمارات الأعمال المدعومة بتقنية المعلومات. كما سنتحدث أيضاً عن أهمية إطار قيمة تقنية المعلومات Val IT في الفصل الثاني والعشرين من هذا الكتاب. وسيصف لنا هذا الفصل أيضاً العلاقة الموجودة

بين أهداف الإطار كوبت وإطار الرقابة الداخلية COSO والذي تم الحديث عنه في الفصل الرابع من هذا الكتاب.

وعلى الرغم من أن الإطار كوبت ظهر في الأصل أداة إرشادية خاصة بتدقيق تقنية المعلومات، فإنه أصبح في الوقت الحالي أكثر اتساعاً وشمولاً. لذا ينبغي أن يكون لدى المسؤولين التنفيذيين اليوم معرفة عالية المستوى برسالة الإطار كوبت وأهدافه، كما ينبغي عليهم أن يكونوا في الموضع الذي يمكنهم من سؤال كل من إدارة تقنية المعلومات والإدارة العامة لعمليات التشغيل المالية لديهم حول استخدام المؤسسة للإطار كوبت في أنشطة حوكمة تقنية المعلومات. فبالإضافة إلى معرفة وفهم إطار الرقابة الداخلية COSO، فإن فهم الإطار كوبت سوف يساعد المدير الأول على تحقيق مستوى فهم أفضل لدور الرقابة وعمليات الحوكمة والمخاطر الخاصة بتقنية المعلومات في العديد من بيئات المؤسسة.

المقدمة التنفيذية للإطار كوبت:

إن كلمة COBIT تعد غير مألوفة أو غريبة بعض الشيء بالنسبة للعديد من الأشخاص، إلا أن هذا المصطلح أصبح متعارفاً عليه بشكل متزايد من قبل مدققي ومحترفي تقنية المعلومات والعديد من مديري المؤسسات. وعلى الرغم من أن هذا الإطار يُعرف الآن اختصاراً باسم COBIT فإنه في الأصل وللسنوات عديدة كان يكتب CobiT: وفي كلتا الحالتين يشير هذا الاختصار إلى أهداف ضوابط المعلومات والتقنيات ذات الصلة (Control Objectives for Information and related Technology). ونظراً لتركيز هذا الإطار على كل من الضوابط والتقنية، فقد تم استخدام الحروف الكبيرة (C و T) في كتابة الحرف الأول والأخير من الاسم المختصر لهذا الإطار. فالإطار كوبت هو إطار للرقابة الداخلية الخاصة بحوكمة تقنية المعلومات وأداة دعم هامة لتوثيق وفهم المتطلبات الخاصة بالضوابط الداخلية للإطار COSO وقانون ساربنز أوكسلي SOX، وإدراك قيمة أصول تقنية المعلومات في المؤسسة والمخاطر المصاحبة لها. لذا يجب على العديد من أعضاء طاقم التدقيق الداخلي أن يكون لديهم على الأقل معرفة عامة أو عملية بالإطار كوبت. كما ينبغي على كبار المديرين في جميع أنحاء المؤسسة أن يكون لديهم معرفة عامة عن الإطار كوبت وأهميته بوصفه أداة لدعم حوكمة تقنية المعلومات.

قام معهد حوكمة تقنية المعلومات (ITGI) ^(١) والمنظمة المهنية الوثيقة الصلة به، وهي جمعية تدقيق وضبط نظم المعلومات (إزاكا) Information Systems Audit and Control Association (ISACA) بإصدار إطار العمل كوبيت والمعايير الخاصة به والتعديل عليها على نحو منتظم. تركز جمعية إزاكا بدرجة كبيرة على عمليات تدقيق تقنية المعلومات، في حين ينصب تركيز معهد ITGI على عمليات البحث والحوكمة. كما تقوم جمعية إزاكا أيضاً بإدارة الاختبارات والتصميم المهني لشهادة مدقق تقنية معلومات معتمد Certified IT Auditor أو مدقق نظم معلومات (CISA)، هذا إلى جانب إدارتها لشهادات أخرى مثل شهادة مدير نظم معلومات معتمد Certified Information Systems Manager (CISM)، وتصميم شهادة وامتحانات معتمد في حوكمة تقنية المعلومات المؤسسية Certified in Governance of Enterprise IT (CGEIT). وتستهدف شهادة مدير أمن معلومات معتمد (CISM) مديري أمن تقنية المعلومات وتعزز من تطوير قدرات المهنيين المحترفين الذين يرغبون في الاعتراف بخبراتهم ومعرفتهم ذات الصلة بحوكمة تقنية المعلومات.

إن العديد من موظفي إدارة تقنية المعلومات والموظفين النظاميين في وحدة التدقيق الداخلي هم أيضاً أعضاء في جمعية إزاكا. ولأسباب تتعلق بالتوق إلى الماضي كانت جمعية إزاكا تُعرَف في الأصل باسم جمعية مدققي نظم معالجة البيانات الإلكترونية EDP Auditors Association (EDPAA)، وهي مجموعة مهنية بدأت في عام ١٩٦٧ من قبل المدققين الداخليين الذين شعروا بأن المنظمة المهنية التابعين لها والتي عُرفت فيما بعد باسم، معهد المدققين الداخليين (IIA) Institute of Internal Auditors، لم تهتم الاهتمام الكافي بأهمية نظم تقنية المعلومات والضوابط التقنية باعتبارها جزءاً من أنشطة الرقابة الداخلية. وقد نسينا أن نذكر أن EDP كانت في يوم من الأيام ترمز إلى Electronic Data Processing أي معالجة البيانات الإلكترونية، أما اليوم فإن هذا المصطلح قد عفا عليه الزمن ولم يعد يُستخدم في مجال تقنية المعلومات، ومع مرور الوقت قامت هذه المؤسسة المهنية بتوسيع نشاطها وأصبحت جمعية إزاكا.

بدأت جمعية مدققي نظم معالجة البيانات الإلكترونية EDPAA - والتي كانت في المقام الأول عبارة عن منظمة مهنية حديثة العهد بمجال تدقيق تقنية المعلومات - في تطوير

مواد إرشادية مهنية خاصة بتدقيق تقنية المعلومات، وقد كان ذلك بعد فترة وجيزة من تأسيسها، وبمجرد أن تطورت جمعية EDPAA إلى جمعية ISACA ثم تحولت في الوقت الحالي إلى معهد ITGI، أصبحت المعايير الأصلية الخاصة بتدقيق تقنية المعلومات الصادرة عنها مجموعة ممتازة من أهداف الرقابة الداخلية والتي تطورت إلى الإطار كويت، وهو الآن بنسخته الخامسة التي أصدرت عام ٢٠١١^(٢). وهذا الإصدار الجديد للإطار لم يكن قد تم نشره بشكل رسمي حتى وقت نشرنا لهذا الكتاب، إلا أننا نستند في حديثنا هنا إلى الإصدارات الخاصة بالمسودة الأخيرة لهذه النسخة على افتراض أنه سيتم قريباً إطلاقها بشكل رسمي. من الناحية العملية، فإن جميع العمليات المؤسسية ترتبط اليوم بموارد تقنية المعلومات، لذا فإن فهم مجال حوكمة تقنية المعلومات بصورة شاملة أصبح أمراً في غاية الأهمية.

ويتكون الإطار كويت مما يطق عليه اسم المبادئ الخمسة five principles، وهي عبارة عن مجالات واسعة ومتداخلة في الحوكمة والضوابط الداخلية، كما هو مبين بالشكل التوضيحي (١-٥). فإن مبادئ الإطار كويت عبارة عن خمسة مجالات رئيسية تتمحور حول أهمية المبدأ الأساسي لحوكمة تقنية المعلومات، وهذه المبادئ هي:

المبدأ الأول لكويت: إطار عمل متكامل لتقنية المعلومات: يدعو الإطار كويت إلى بذل الجهود اللازمة لكي تتماشى عمليات تشغيل تقنية المعلومات وأنشطتها مع جميع عمليات التشغيل الأخرى في المؤسسة. وهذا يشمل إيجاد الروابط بين عمليات تشغيل الأعمال وخطط تقنية المعلومات في المؤسسة، هذا بالإضافة إلى وضع عمليات لتحديد العلاقات بين الجودة والقيمة والمحافظة عليها والتأكد من صحتها.

المبدأ الثاني لكويت: دوافع تحقيق القيمة لأصحاب المصلحة: يجب أن يكون هناك عمليات متعارف عليها لضمان تقديم وحدة تقنية المعلومات ووحدات التشغيل الأخرى في المؤسسة للقيم والفوائد المرجوة من خلال الدورة الخاصة بتقديمها وباستخدام الإستراتيجية التي تقلص التكاليف مع التأكيد على القيم الذاتية المكتسبة من أنشطة تقنية المعلومات وغيرها من الأنشطة الخاصة بالمؤسسة.

المبدأ الثالث لكويت: تركيز الموارد على بيئة أو سياق الأعمال: مع التركيز على تقنية المعلومات، يجب أن تكون هناك استثمارات مناسبة، وإدارة سليمة، للعناصر الهامة في تقنية

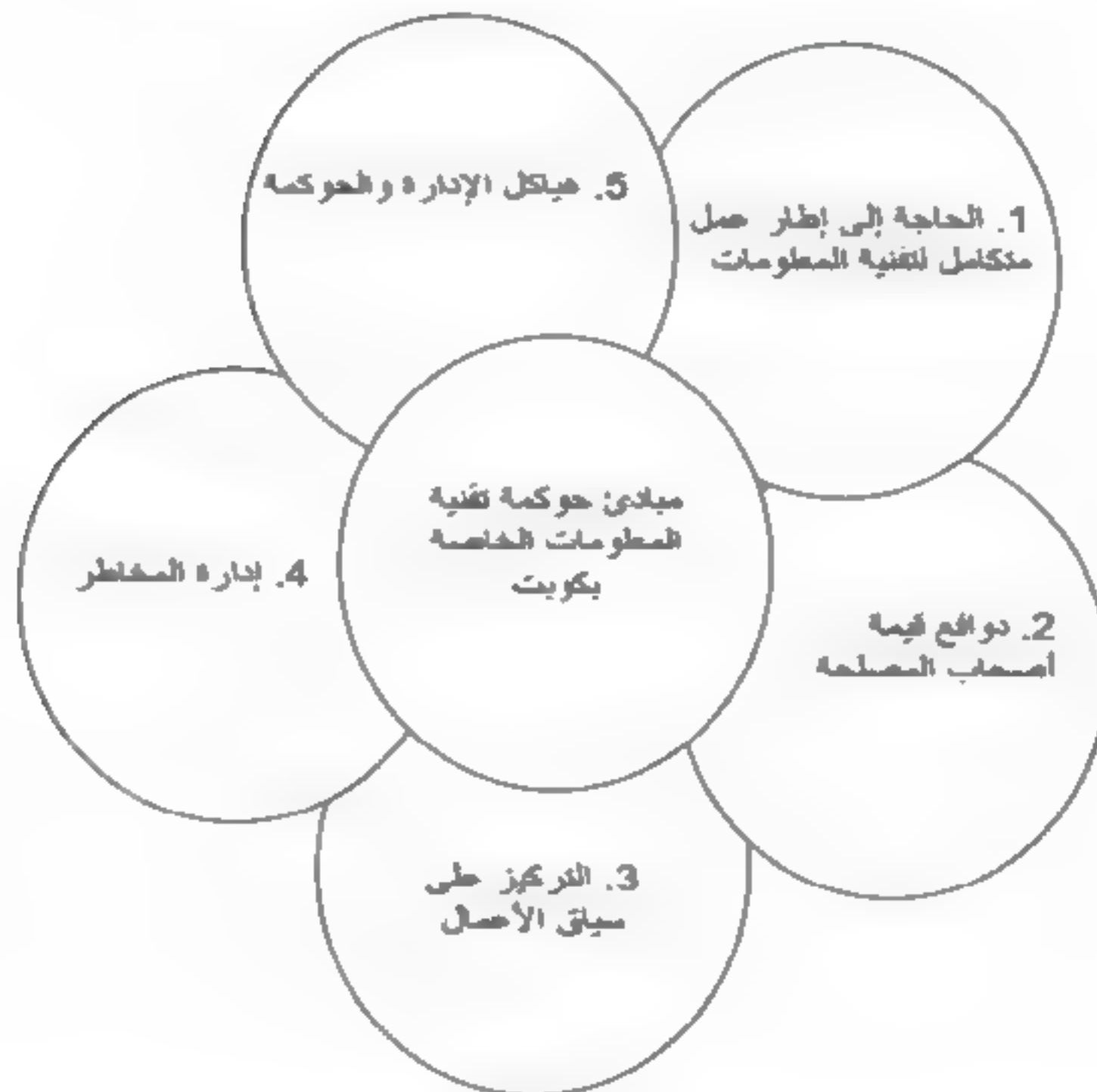
المعلومات من موارد وتطبيقات ومعلومات وبنى تحتية وأفراد. حيث تعتمد الحوكمة الفعالة لتقنية المعلومات على هذا التحسين في المعرفة والبنية التحتية.

المبدأ الرابع لكوبت: إدارة المخاطر: ينبغي أن يكون لدى الإدارة، وعلى جميع المستويات، فهم واضح لمدى رغبة المؤسسة في المخاطر أو ما يعرف بـ Risk Appetite، ومتطلبات الامتثال الخاصة بها، وتأثير المخاطر الكبيرة. فلكل من إدارة تقنية المعلومات وغيرها من الإدارات الأخرى مسئولياتها الخاصة والمشاركة لإدارة المخاطر التي قد تؤثر بشكل فردي أو جماعي على المؤسسة بأكملها.

المبدأ الخامس لكوبت: قياس الأداء: ينبغي أن تكون هناك عمليات متعارف عليها ومعمول بها لمتابعة ومراقبة تنفيذ الإستراتيجية واكتمال المشروع واستخدام الموارد وأداء العمليات وتقديم الخدمات. كما ينبغي أن تقوم آليات حوكمة تقنية المعلومات بترجمة إستراتيجيات التنفيذ إلى إجراءات ومقاييس لتحقيق تلك الأهداف.

شكل توضيحي (١-٥)

مبادئ كوبت الخاصة بحوكمة تقنية المعلومات



هذه هي المبادئ أو مناطق التركيز الخمسة الخاصة بكوبت التي تحدد عناصره وتقدم تعريفاً للعناصر الأساسية لحوكمة تقنية المعلومات. يعتبر الإطار كوبت من الأدوات الفعالة لتوثيق ضوابط تقنية المعلومات وجميع الضوابط الداخلية الأخرى، وينظر هذا الفصل إلى الإطار كوبت من منظور أشمل لاستخدامه للمساعدة في عمليات حوكمة تقنية المعلومات الخاصة بالإدارة والمؤسسة ووحدة التدقيق الداخلي.

تقدم الأجزاء التالية من هذا الفصل وصفاً شاملاً للإطار كوبت، في الصيغة النهائية لمسودة الإصدار الحالي وهو الإصدار الخامس، وعناصره الرئيسية التي تقوم بربط الأعمال مع أهداف تقنية المعلومات من خلال الضوابط الرئيسية ومعايير القياس الفعالة. إضافة إلى أن هذا الفصل سوف يقوم بوصف معايير كوبت مع ما يناظرها في إطار الرقابة الداخلية COSO، والذي تمت مناقشته في الفصل الرابع من هذا الكتاب، وأفضل الممارسات الخاصة بمكتبة البنية التحتية لتقنية المعلومات، التي تم تقديمها في الفصل السادس من هذا الكتاب، والحوكمة الشاملة لتقنية المعلومات والشركات. كما سيتم مناقشة العناصر والمكونات الرئيسية لحوكمة تقنية المعلومات. يعد الإطار كوبت إحدى الآليات الفعالة لتوثيق وفهم الضوابط الداخلية وإدارة عمليات حوكمة تقنية المعلومات على جميع المستويات. وعلى الرغم من أن كوبت كان في البداية عبارة عن مجموعة من المواد الإرشادية الخاصة بـ "تدقيق تقنية المعلومات" فإنه اليوم أصبح أداة أكثر قوة.

إطار العمل كوبت والعوامل المحركة له:

تعد عمليات تقنية المعلومات والتطبيقات البرمجية والأجهزة المادية الداعمة لها من المكونات الرئيسية لأي مؤسسة في الوقت الراهن. فسواء كانت هذه المؤسسة من المؤسسات الصغيرة التي تقوم بممارسة عمليات البيع بالتجزئة التي لها احتياجات بسيطة كمتابعة المخزون ودفع رواتب الموظفين، أم كانت من المؤسسات الكبيرة جداً ضمن تصنيف أفضل خمسين مؤسسة أو "Fortune 50"، فجميعها يحتاج إلى مجموعة كبيرة من عمليات تقنية المعلومات المترابطة والمعقدة أحياناً والتي ترتبط ارتباطاً وثيقاً بعمليات تشغيل الأعمال المتعلقة بها. بمعنى أنه، ينبغي أن يعمل كل من عمليات الأعمال وموارد تقنية المعلومات الداعمة لها في المؤسسة ضمن علاقة وثيقة لتبادل

المعلومات. لا يمكن لتقنية المعلومات - وبالتأكيد لا ينبغي - أن تكشف لعمليات تشغيل الأعمال عن الأنواع الخاصة بعمليات ونظم تقنية المعلومات التي ينبغي عليها تنفيذها، ولكنها تقوم بتوفير المعلومات التي تؤثر في قرارات تلك الأعمال. في الأيام الأولى لظهور نظم الحاسبات، شعر المديرون في بعض الأحيان، بأنهم يملكون العديد من الإجابات والحلول المطورة للنظم المتعلقة بأعمالهم، إلا أنها أحياناً كانت تأتي بنتائج عكسية تماماً. ومع ذلك، فإن هذه العلاقة قد تغيرت منذ فترة طويلة؛ فبوجه عام ينبغي أن تكون هناك علاقة وثيقة لتبادل المعلومات والمتطلبات المشتركة بين عمليات تشغيل تقنية المعلومات وعمليات تشغيل الأعمال. وينبغي على مدير المؤسسة فهم الاحتياجات والمتطلبات اللازمة لتبادل المعلومات بين الطرفين. فتقنية المعلومات لديها مسئوليات تजाة المجالات الأخرى المرتبطة بالعملية التي يتم تدقيقها من قبل أو من خلال إرشادات التدقيق المعتمدة، التي يتم قياسها من خلال سلسلة من القياسات والأنشطة الخاصة بمؤشر الأداء، التي يتم تفعيلها من خلال أهداف النشاط. كل ذلك أصبح جزءاً لا يتجزأ من كويت الذي يعد إطاراً لحوكمة وضبط تقنية المعلومات ويحدد أهداف أفضل الممارسات والحوكمة والرقابة الداخلية لكل عملية من عمليات تقنية المعلومات والأعمال.

فبالإضافة إلى إطار الرقابة الداخلية COSO ومتطلبات الضوابط الداخلية لقانون ساربنز أوكسلي SOX، يقدم هذا الفصل الإصدار الخامس والجديد لكويت. وقد يتساءل أحد المسؤولين التنفيذيين للمؤسسة قائلاً: "أعتقد أنني أفهم بعض القواعد الرئيسية لقانون ساربنز أوكسلي SOX، وأن مؤسستي تقوم باستخدام إطار الرقابة الداخلية COSO؛ فلماذا يجب علي الاهتمام بهذا الشيء المسمى كويت، واعتماده كإطار آخر؟" إن إجابتنا عن هذا التساؤل هي أن كويت يوفر نهجاً بديلاً بل وأحياناً مفضلاً لتعريف ووصف العمليات التي تركز على حوكمة تقنية المعلومات بصورة أكثر من الإطار التقليدي للرقابة الداخلية COSO. في هذه الأيام تعتبر المعلومات والعمليات الداعمة لتقنية المعلومات هي بالفعل الأصول الأكثر أهمية وقيمة بالنسبة لجميع المؤسسات. وتقع على عاتق الإدارة مسؤولية كبيرة وهي الحفاظ على الأصول الداعمة لتقنية المعلومات، متضمناً ذلك النظم الآلية. ويحتاج المسؤول التنفيذي في المؤسسة هذه الأيام إلى فهم هذه العمليات المرتبطة

بالمعلومات والضوابط الداعمة لها. وتهتم هذه التركيبة بفاعلية وكفاءة جميع الموارد والعمليات والمتطلبات الشاملة لأعمال تقنية المعلومات الخاصة بها.

يقر الإطار كوبت بأن المعلومات يجب أن تكون أحد الموارد الرئيسية لجميع المؤسسات، حيث إن هناك اعتمادية هائلة على التقنية طيلة دورة حياة المعلومات بالكامل. حيث تنتشر تقنية المعلومات والتقنيات المرتبطة بها في المؤسسات، وهي بحاجة إلى أن تُحكم وتدار بطريقة شمولية، مع أخذ كامل المسؤولية المتعلقة بجميع مجالات الأعمال ومهام تقنية المعلومات بصورة تامة (من النهاية إلى النهاية). فمن خلال التنفيذ الفعال لإرشادات الإطار كوبت. يجب على المؤسسة أن تحقق المزيد من:

- إيجاد القيمة من خلال تقنية المعلومات المؤسسية.
- رضا مستخدمي الأعمال عن الأعمال والخدمات التي تقدمها تقنية المعلومات.
- الالتزام بالقوانين واللوائح والسياسات ذات العلاقة.

وكما ذكرنا، فقد استمر تطوير وتحسين الإطار كوبت على مر السنين. وقد اعتمدنا في تعليقاتنا في هذا الفصل في المقام الأول على الإصدار الخامس الجديد الذي كان في مسودة النهائية أثناء القيام بتأليف هذا الكتاب. كما سنقوم أيضاً بتضمين بعض المراجع التي تشير إلى الإصدار السابق للإطار كوبت - الإصدار ٤,١ - والمُعترف به على نحو جيد. إن النسخة الجديدة كوبت ٥,٠ (COBIT 5.0) تعد تحسناً كبيراً للنسخة السابقة، كما أنها توفر دعماً وإرشادات ممتازة لتحسين عمليات حوكمة تقنية المعلومات، ورغم أنه قد تكون هناك بعض التعديلات النهائية عندما يتم إطلاق الإصدار الخامس بشكل رسمي، فإن العديد من الأوصاف التي استخدمناها للإطار كوبت توحى بأنه سيتم إطلاق الإصدار الجديد والنهائي قريباً. واستناداً إلى مبادئ كوبت الخاصة بحوكمة تقنية المعلومات والموضحة في الشكل التوضيحي (٥-١)، فإن الأقسام التالية سوف تقدم مستوى رفيعاً ونظرة تنفيذية عامة لكوبت، ولماذا يعد هذا الإطار من الأدوات الهامة في حوكمة تقنية المعلومات.

المبدأ الأول لكوبت: إنشاء إطار متكامل لبنية تقنية معلومات:

تصف البنية المعمارية كيف نقوم ببناء المقر الرئيسي الخاص بمكتبنا أو النمط المستخدم في بنائه، إلا أنها هذه الأيام تستخدم غالباً للإشارة أيضاً إلى الاختيارات التقنية لبنية تقنية المعلومات في المؤسسة. فعلى سبيل المثال، عندما تحولت إدارت تقنية المعلومات من نظم الحاسبات المركزية القديمة التي كانت موجودة منذ عدة سنوات إلى الشبكات التي تحتوي على خوادم أصغر حجماً، فقد أعلنت إدارة تقنية المعلومات في المؤسسة بأنها اعتمدت وطبقت البنية التي تدعى "العميل - الخادم". وتستخدم إدارت تقنية المعلومات مصطلح بنية أو معمارية النظم لتشير إلى الشكل العام للأجهزة المادية أو البرمجيات الخاصة بموارد تقنية المعلومات لديها. يمتلك كوبت أيضاً البنية أو المعمارية الخاصة به؛ ومع ذلك، فإن النسخة المنشورة الحالية لبنية كوبت (كوبت ٥,٠) قد تخيف غير المتخصصين في تقنية المعلومات بسبب تعقيدية الرسم التخطيطي للإطار في مسودته الحالية. الشكل التوضيحي (٥-٢) عبارة عن رسم تخطيطي مبسط لمكونات البنية المعمارية الخاصة بالإصدار الخامس لكوبت (كوبت ٥,٠).

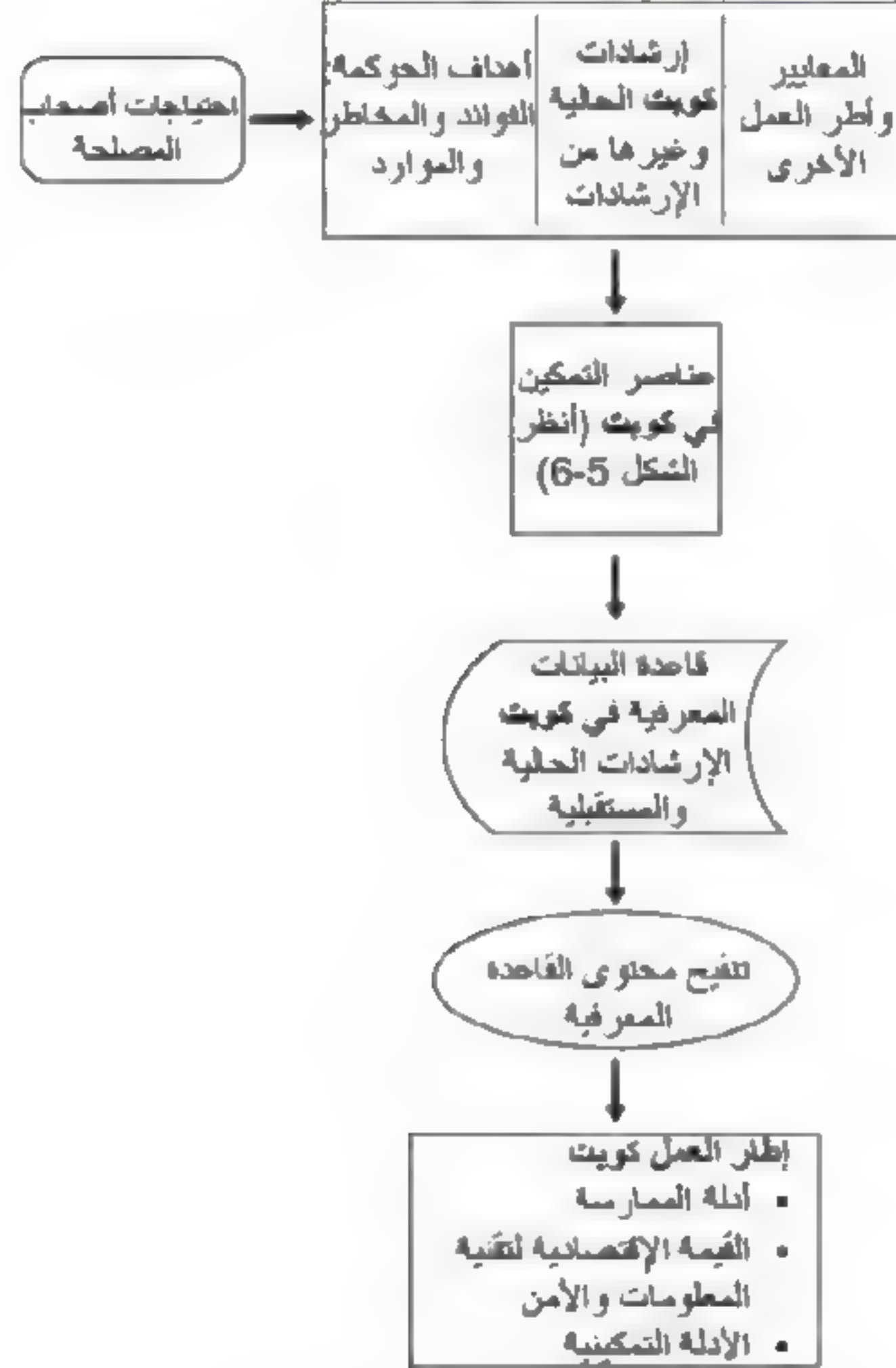
وبالرجوع إلى معمارية كوبت والعودة إلى خطوات بدايته، نجد أن المبدأ المهم هنا هو أن عمليات كوبت والعمليات الأخرى التي تخص حوكمة تقنية المعلومات تكون مدفوعة باحتياجات أصحاب المصلحة بدءاً من الإدارة العليا التي تأمل في تحسين عمليات حوكمة تقنية المعلومات، والتي ربما تكون من خلال الإدارة المحلية لتقنية المعلومات التي ترغب هي الأخرى في تحسين عمليات محددة في تطبيقاتها. ويكون أصحاب المصالح عادة عبارة عن مجموعات كبيرة ومختلفة يتشاركون ويختلفون أحياناً في بعض الاهتمامات والأمر التي تتعلق بعمليات حوكمة تقنية المعلومات في المؤسسة. ويتم تقديم هذه الاهتمامات أو الاحتياجات إلى العمليات المعتمدة لكوبت، مع التركيز على أهداف حوكمة وقيمة تقنية المعلومات. أضف إلى ذلك أن كوبت لا يمكن الاعتماد عليه بمفرده، إذ لا بد من تنسيق هذه الاحتياجات مع المعايير والأطر والعمليات الأخرى الموجودة في المؤسسة.

وكما هو موضح في الشكل التوضيحي (٥-٢)، فإن هذه الاحتياجات تتحقق من خلال العناصر التي يطلق عليها كويت اسم "عناصر التمكين"، وهي عبارة عن سلسلة من العمليات المنفصلة والمتراصة والتي سنتطرق إليها لاحقاً في هذا الفصل. والغرض من عناصر التمكين هذه هو - كما يشير إليه الاسم - تنفيذ وتطبيق العمليات الخاصة بنظم حوكمة وإدارة تقنية المعلومات المؤسسية. وقد تم تعريف عناصر التمكين بشكل موسع على أنها عمليات أو آليات محددة، أو أي شيء يمكن أن يساعد في تحقيق أهداف الحوكمة المؤسسية. ويشمل ذلك موارد كالمعلومات والأفراد. يحدد إطار كويت ٥,٠ سبع فئات من عناصر التمكين هي:

- ١- العمليات
- ٢- المبادئ والسياسات.
- ٣- الهياكل التنظيمية.
- ٤- المهارات والكفاءات.
- ٥- الثقافة والسلوك.
- ٦- القدرات الخدمية.
- ٧- المعلومات.

شكل توضيحي (٢-٥)

البنية العامة المبسطة لكوبت ٥



تتفاعل هذه العناصر التمكينية معاً بطريقة منتظمة، وهذا يعني أن نظام الحوكمة والإدارة لا يمكن أن ينجح إلا إذا تم تناول جميع عناصر التمكين والتعامل معها وفهم التفاعلات الرئيسية الخاصة بها. وسنقوم لاحقاً في هذا الفصل بمناقشة عناصر التمكين الخاصة بكوبت.

بعد ذلك ستقوم عناصر التمكين المستخدمة بتوفير الدعم اللازم لقاعدة البيانات المعرفية لكوبت، والتي تتضمن المواد الإرشادية الحالية والهياكل الخاصة بالأنشطة المستقبلية. وسيسهم كل ذلك في تقديم الدعم المناسب لتطبيق جميع عمليات الإطار

كويت والمدعومة أيضا بواسطة مجموعة من الإرشادات المتعلقة بالمنتجات والإرشادات المرجعية. إن فكرة البنية المعمارية لكويت أو الفائدة المرجوة منها هي دعم أهداف إطار العمل من خلال تزويد جميع أصحاب المصلحة بالإرشادات الأكثر اكتمالاً وحدثة، وهي تتعلق بحوكمة وإدارة تقنية المعلومات المؤسسية. ولتحقيق هذه الفائدة، فإن البنية المعمارية لكويت تضم مجموعة واسعة من المكونات الآلية والمكونات المتعلقة بالبيانات، مثل المواد الإرشادية التي تحدثنا عنها في فصول أخرى. وسيتم لاحقاً في هذا الفصل مناقشة الغرض من هذه العناصر التمكينية ووظيفتها بمزيد من التفاصيل.

كويت هو مجموعة من المواد التوجيهية التي تدعم العناصر الرئيسية للإرشادات الخاصة بحوكمة تقنية المعلومات، والتي تتضمن العديد من المفاهيم والموضوعات المتعلقة بالتقنيات الخاصة بحوكمة وإدارة المؤسسة. لقد قامت المؤسسات بمختلف أحجامها وفي جميع أنحاء العالم بتطبيق كويت بنسخته السابقة ٤,١. أما الإصدار الجديد لكويت (كويت ٥,٠) فإنه يقدم تحسينات للحد من المخاطر المتعلقة بتقنية المعلومات وزيادة الثقة في المعلومات التي تقدمها تقنية المعلومات، لتمكين من تطوير سياسة واضحة وممارسات جيدة لإدارة تقنية المعلومات، وزيادة القيمة المكتسبة من تقنية المعلومات وإدارة الامتثال.

المبدأ الثاني لكويت: دوافع تحقيق قيمة لأصحاب المصلحة:

يتحقق تركيز عمل كويت من خلال تحديد جميع أصحاب المصلحة واحتياجاتهم وتحديد الكيفية التي يرتبطون بها مع قرارات وأنشطة الحوكمة والإدارة. ولنا أن نتصور أن أصحاب المصلحة المستفيدين من عملية تقنية المعلومات وعمليات تشغيلها منقسمون إلى مجموعتين: داخليين وخارجيين. وإن عمليات تشغيل وعمليات تقنية المعلومات منتشرة بشكل كبير، وإن مجموعة أصحاب المصالح الداخليين الذين تم تحديدهم من خلال كويت تشمل أعضاء مجلس الإدارة، الرئيس التنفيذي CEO، المدير المالي (CFO)، المدير التنفيذي للمعلومات (CIO) ومديري الأعمال التنفيذيين، وأصحاب عمليات الأعمال، ومديري الأعمال، ومديري المخاطر، ومديري الأمن ومديري الخدمات، ومديري الموارد البشرية (HR) والمدققين الداخليين ومستخدمي تقنية المعلومات، ومديري عمليات تشغيل تقنية المعلومات، وغيرهم الكثير. وسيكون لكل من هؤلاء توقعات ومواقف مختلفة حول القضايا

الخاصة بحوكمة تقنية المعلومات. والشكل التوضيحي (٣-٥) يلخص بعض الاحتياجات النمطية لأصحاب المصلحة الداخليين وفقاً للإطار كوبت.

شكل توضيحي (٣-٥)

الاحتياجات القياسية لأصحاب المصلحة الداخليين طبقاً لكوبت

- في ضوء أمن تقنية المعلومات، والمخاوف المتعلقة بالخصوصية، وغيرها من القضايا، هل قمنا بتناول جميع المخاطر ذات الصلة بتقنية المعلومات؟
- هل نقوم بتنفيذ عمليات تشغيل فعالة ومرنة لتقنية المعلومات؟
- كيف يمكننا ضبط تكاليف تقنية المعلومات بشكل أفضل؟
- كيف يمكننا استخدام موارد تقنية المعلومات بالأسلوب الأكثر فاعلية وكفاءة؟
- ما خياراتنا الأكثر فاعلية وكفاءة لتوريد معدات تقنية المعلومات؟
- هل لديّ ما يكفي من الأفراد لتشغيل وإدارة تقنية المعلومات، وكيف يمكنني تطوير والحفاظ على مهاراتهم وإدارة أدائهم؟
- كيف نحصل على ضمانات بشأن نتائج وأداء عمليات تقنية المعلومات؟
- هل المعلومات التي نقوم بمعالجتها مؤمنة بشكل جيد؟
- كيف لنا أن نقوم بتحسين مرونة الأعمال من خلال بيئة تقنية معلومات أكثر مرونة؟
- هل جميع مستويات الإدارة وعمليات التشغيل على بصيرة بما تقوم به تقنية المعلومات؟
- هل تفشل مشروعات تقنية المعلومات كثيراً في تحقيق ما وعدت به؟
- إلى أي مدى تكون تقنية المعلومات هامة لاستمرارية المؤسسة؟
- كيف لنا أن نعرف أن تقنية المعلومات وعمليات التشغيل ذات الصلة الخاصة بشركاء الأعمال لدينا آمنة ويمكن الاعتماد عليها؟
- كيف لي أن أعرف أن المؤسسة متوافقة مع القوانين واللوائح المعمول بها؟
- كيف لنا أن نعرف إذا كانت المؤسسة تحافظ على نظام فعال للرقابة الداخلية؟

كما تضم مجموعة أصحاب المصالح الخارجيين كلاً من شركاء العمل والموردين والمساهمين والجهات التنظيمية أو التشريعية (الحكومة) والمستخدمين الخارجيين والعملاء ومنظمات المعايير القياسية والمدققين الخارجيين والاستشاريين والعديد من الجهات الأخرى المعنية بعمليات وموارد تقنية المعلومات. وتشمل احتياجات أصحاب المصلحة الخارجيين أسئلة مثل:

- كيف يمكنني معرفة ما إذا كانت عمليات شريكي في العمل آمنة ويمكن الاعتماد عليها؟
- كيف يمكنني معرفة ما إذا كانت هذه المؤسسة ووحداتها التنظيمية متوافقة مع القواعد واللوائح المعمول بها؟
- كيف لي أن أعرف ما إذا كانت المؤسسة تحافظ على نظام فعال للرقابة الداخلية؟

هناك عدة دوافع يمكن أن تؤثر في احتياجات أصحاب المصلحة منها التغييرات التي تطرأ على الإستراتيجية، والأعمال، والبيئة التنظيمية، والتطورات التقنية. وتتجسد احتياجات أصحاب المصلحة هذه في سلسلة من التوقعات أو المخاوف أو المتطلبات المحتملة؛ كل هذه القضايا ترتبط بواحد أو أكثر من أهداف الحوكمة الثلاثة العامة الخاصة بكويت، وهي: تحقيق الفوائد وموازنة المخاطر وتحسين التكلفة.

إن الغرض من وجود المؤسسات هو إيجاد قيمة لأصحاب المصلحة لديها. ومن ثم فإن هدف الحوكمة لأية مؤسسة - تجارية أو غير تجارية - هو إيجاد القيمة وتحقيق فوائد بتكلفة مثالية للموارد مع الحد من المخاطر. فالمؤسسات لديها العديد من أصحاب المصلحة الداخليين والخارجيين. و"إيجاد القيمة" يعني أشياء مختلفة - وأحياناً متعارضة - لكل منهم. فالحوكمة عبارة عن التفاوض واتخاذ القرارات بشأن تقديم الحلول والتوفيق بين المصالح المختلفة لأصحاب المصلحة فيما يخص تحقيق هذه القيمة. ومن ثم فإنه يجب أن يقوم نظام حوكمة تقنية المعلومات بالنظر إلى جميع أصحاب المصلحة عند القيام بعمل تقييمات واتخاذ قرارات بشأن الفوائد والموارد والمخاطر. إن السؤال الذي يمكن، بل وينبغي أن يطرح لكل عنصر من هذه العناصر الخاصة بإيجاد القيمة هو: لمن ستكون الفوائد والمخاطر؟ وما الموارد المطلوبة لتقنية المعلومات؟

المبدأ الثالث لكوبت: التركيز على سياق الأعمال:

كما ذكرنا في تعليقاتنا السابقة، بدأ كوبت في الأساس أداة لتدقيق تقنية المعلومات، فهو عبارة عن مجموعة محسنة من العمليات الموصى بها لمراجعة وتقييم إجراءات الرقابة الداخلية الخاصة بتقنية المعلومات. كيف تغيرت الأشياء على مر السنين؟ ففي الوقت الراهن، يقوم الإطار كوبت بتوفير مجموعة قوية من المواد الإرشادية التي تساعد المؤسسة على تحسين عمليات حوكمة تقنية المعلومات، فالمبدأ الأساسي لكوبت هو التركيز على سياق الأعمال.

يؤكد المبدأ الرئيسي الثالث لكوبت أن الغرض من وجود المؤسسات هو خلق أو إيجاد قيمة لأصحاب المصلحة. وهناك ثلاثة أهداف لقيمة الحوكمة المعرفة من قبل كوبت هي:

١- تحقيق الفوائد.

٢- تحسين المخاطر.

٣- تحسين الموارد.

يعمل كوبت على ربط كل هدف من هذه الأهداف الثلاثة بالأهداف المالية والأهداف المتعلقة بخدمة العملاء والأهداف الداخلية في المؤسسة. يقوم كوبت أيضاً بتحديد مجموعة من الأهداف المالية للمؤسسة، والتي تم تقسيمها إلى عدة فئات من الأهداف المؤسسية أي الأهداف المالية، وأهداف العملاء، والأهداف الداخلية، والأهداف الخاصة بالتعلم والنمو. الشكل التوضيحي (٥-٤) يعرض ملخصاً لأهداف الحوكمة في كوبت مقابل الأهداف المالية للمؤسسة من حيث كونها علاقة رئيسة أو ثانوية مع أهداف قيمة الحوكمة المعرفة من قبل كوبت.

شكل توضيحي ٤-٥

ملخص أهداف الحوكمة في كويت مقابل الأهداف المؤسسية

أهداف الحوكمة			أهداف المؤسسة	
تحسين الموارد	تحسين المخاطر	تحقيق الفوائد		
		ر	١. القيمة المتحققة لأصحاب المصلحة من استثمارات الأعمال	المالية
ث		ر	٢. محفظة من المنتجات والخدمات التنافسية	
ث	ر		٣. إدارة مخاطر الأعمال (وقاية الأصول)	
	ر		٤. التوافق مع القوانين والقواعد التنظيمية الخارجية	
ث	ث	ر	٥. الشفافية المالية	
ث		ر	٦. ثقافة خدمية موجهة نحو العميل	العميل
	ر		٧. استمرارية خدمات الأعمال وإتاحتها	
ث		ر	٨. مرونة الاستجابة للتغيرات في بيئة العمل	
ر	ر	ر	٩. اتخاذ القرار الاستراتيجي استناداً إلى المعلومات	
		ر	١٠. تحسين تكاليف تقديم الخدمات	
ر		ر	١١. تحسين الأداء الوظيفي لعمليات الأعمال	الداخلية
ر	ر	ر	١٢. تحسين تكاليف عمليات الأعمال	
ث		ر	١٣. إدارة برامج التغيير في بيئة العمل	
ر	ر		١٤. الإنتاجية التشغيلية وإنتاجية طاقم العمل	
	ث	ث	١٥. التوافق مع السياسات الداخلية	
ر		ر	١٦. أفراد ذوو مهارة ومتحمسون	النمو
		ر	١٧. ثقافة الابتكار في المنتجات والأعمال	

أما الشكل التوضيحي (0-0) فما هو إلا وثيقة أكثر تفصيلاً للغرض من الأهداف المالية. حيث تُظهر المواد الأصلية المنشورة لكوبت علاقات أكثر تفصيلاً لكل هدف من الأهداف الثلاثة للحوكمة، كل واحد منها مقابل الأهداف المؤسسية.

هذه المقابلة التفصيلية تساعد على وصف المبدأ الثالث لكوبت الذي يركز على سياق الأعمال، ويتعين على هذه العلاقات أن تساعد الإدارة على مختلف مستوياتها وكذلك أعضاء طاقم العمل على فهم العلاقات والروابط الموجودة بين عمليات تقنية المعلومات وكل من أنشطة الأعمال الداخلية والخارجية على نحو أفضل.

شكل توضيحي (0-0)

مقابلة الأهداف المالية التفصيلية للحوكمة في كوبت مع الأهداف المؤسسية

الأهداف المالية للمؤسسة					أهداف تقنية المعلومات المؤسسية	
الشفافية المالية	القيمة المتحققة لأصحاب المصلحة من استثمارات الأعمال	محفظة من المنتجات والخدمات التنافسية	إدارة مخاطر الأعمال (حماية الأصول)	التوافق مع القوانين والقواعد التنظيمية الخارجية		
٥	٤	٣	٢	١		
	ر	ر	ث		١. القيمة المتحققة لأصحاب المصلحة من استثمارات الأعمال	المالية
	ث		ث	ر	٢. محفظة من المنتجات والخدمات التنافسية	
	ر	ث	ث		٣. إدارة مخاطر الأعمال (وقاية الأصول)	
			ر	ث	٤. التوافق مع القوانين والقواعد التنظيمية الخارجية	
	ر	ر			٥. الشفافية المالية	

	ث		ث		٦. ثقافة خدمية موجهة نحو العميل	العميل
ر	ر	ر	ث	ث	٧. استمرارية خدمة الأعمال وإتاحتها	
	ث	ث	ث		٨. مرونة الاستجابة للتغيرات في بيئة العمل	
	ث	ر	ث		٩. اتخاذ القرار الإستراتيجي استناداً إلى المعلومات	
			ر	ر	١٠. تحسين تكاليف تقديم الخدمات	
	ر	ر			١١. تحسين الأداء الوظيفي لعمليات الأعمال	الداخلية
	ث	ث	ث		١٢. تحسين تكاليف عمليات الأعمال	
	ر	ث	ث		١٣. إدارة برامج التغيير في بيئة العمل	
	ث	ر	ث	ث	١٤. الإنتاجية التشغيلية وإنتاجية طاقم العمل	
			ث	ث	١٥. التوافق مع السياسات الداخلية	
	ث	ث	ر		١٦. أفراد ذوو مهارة ومتحمسون	النمو
	ث	ر			١٧. ثقافة الابتكار في المنتجات والأعمال	

المبدأ الرابع لكوبت: عناصر تمكين إدارة المخاطر والحوكمة:

كما هو واضح في الوصف الموجز الذي قدمناه للبنية المعمارية لكوبت، فإن عناصر التمكين تعد من العناصر الرئيسية في عملية الحوكمة الخاصة بكوبت. فهي عبارة عن العناصر الملموسة وغير الملموسة التي تجعل شيئاً ما يعمل، وفي هذه الحالة فإن هذا الشيء هو حوكمة وإدارة تقنية المعلومات في المؤسسة. تُظهر البنية العامة المبسطة "لكوبت ٥.٠" في الشكل التوضيحي (٥-٢) وظيفة تسمى عناصر التمكين في وسط العملية الشاملة، التي لا بد أن تتبناها المؤسسة لتتمكن من حوكمة تقنية المعلومات.

وقد حدد كوبت سبعة أصناف أو أنواع مختلفة من عناصر التمكين. كما هو موضح بصورة منفصلة في الشكل التوضيحي (٥-٦). فلكي تحقق المؤسسة أهدافها الرئيسية فإنه يتوجب عليها أن تدرك دائماً بأنها تقوم بإدارة مجموعة مترابطة من عناصر التمكين التي تمتلكها. ويعرض الشكل الخاص بالبنية العامة سبع فئات من عناصر التمكين المترابطة. فعناصر التمكين التي حددها كوبت هي:

- ١- **العمليات:** هي تلك المجموعات المنظمة من الممارسات والأنشطة التي تحقق أهدافاً معينة وتنتج مجموعة من المخرجات لدعم الأهداف الشاملة المتعلقة بتقنية المعلومات.
- ٢- **الثقافة والاخلاقيات والسلوك:** إن الثقافة القوية للمؤسسة إلى جانب التركيز على أخلاقيات العمل وسلوكيات أصحاب المصلحة الداعمة لتلك القيم يتم التقليل من شأنها غالباً إلا أنها من عوامل التمكين الهامة لنجاح أنشطة الحوكمة والإدارة.
- ٣- **الهيكل التنظيمية:** تعتبر الأنشطة والسياسات والترتيبات التنظيمية بمثابة الوسائل الرئيسية لصنع القرار في المنظمة.
- ٤- **المعلومات:** تكون مهمة نظراً لأنها العنصر المنتشر في جميع أنحاء أي منظمة، فالمعلومات ضرورية للحفاظ على تشغيل المنظمة وحوكمتها بشكل جيد، ولكن على المستوى التشغيلي فإن المعلومات تكون غالباً هي المنتج الرئيسي للمؤسسة نفسها.
- ٥- **المبادئ والسياسات:** تعد عناصر التمكين هذه وسيلة لترجمة السلوكيات المرغوب فيها إلى إرشادات عملية للإدارة اليومية.

٦- المهارات والكفاءات: وترتبط هذه السمات بالعناصر البشرية وهي ضرورية لإتمام جميع النشاطات بنجاح واتخاذ القرارات الصحيحة.

٧- القدرات الخدمية: يشتمل هذا العنصر التمكيني على البنية التحتية والتقنية والتطبيقات التي توفر للمؤسسة معالجة المعلومات وتقديم الخدمات.

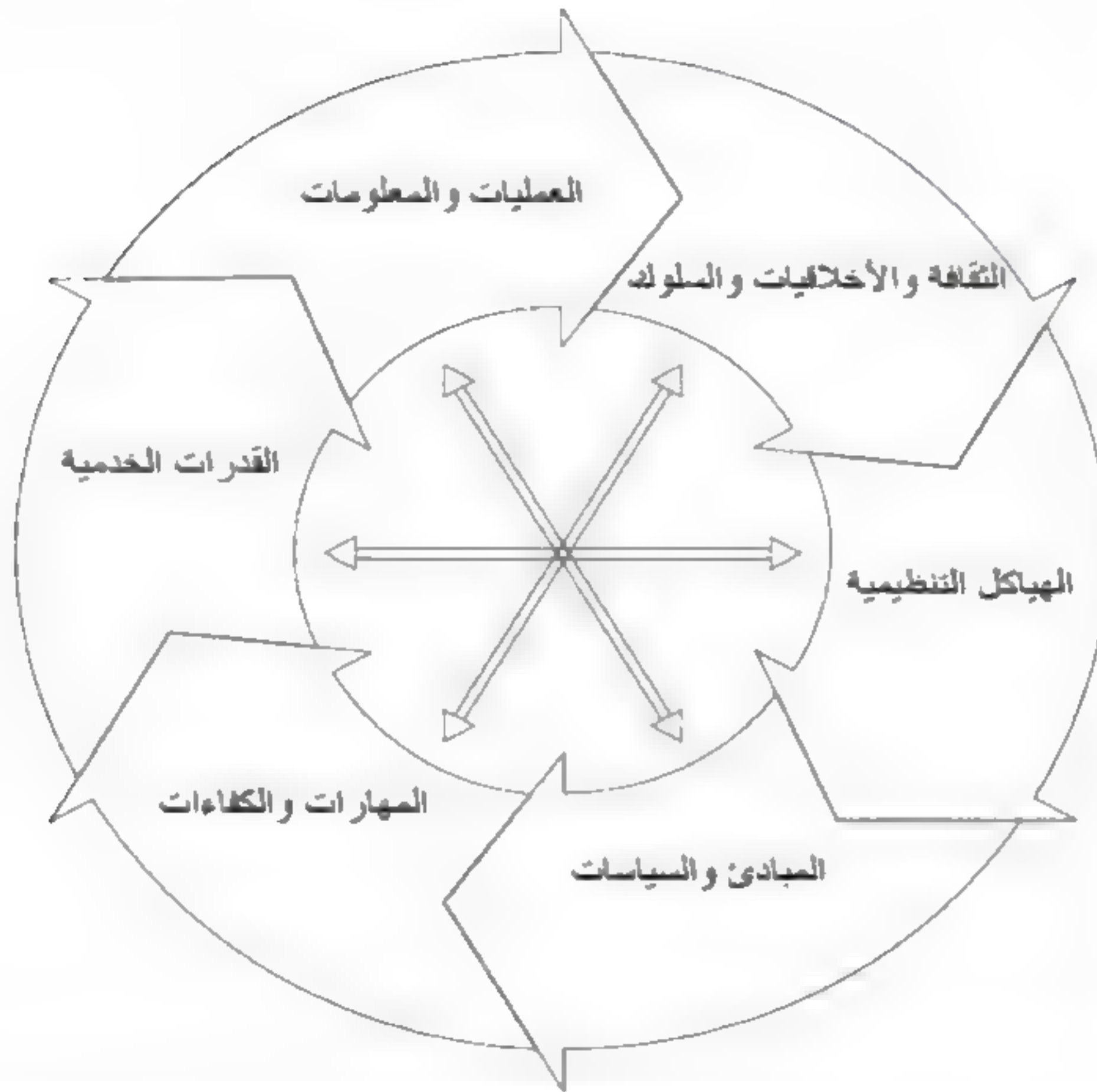
لا يمكن تواجد أي عنصر من عناصر التمكين السبع تلك بشكل منفرد فجميعها بحاجة إلى مدخلات من عناصر تمكين أخرى والتي حددها كويت لكي تكون فعالة بشكل كامل. فمثلاً نجد أن العمليات تحتاج إلى عنصر تمكين المعلومات، والهيكل التنظيمية تحتاج إلى عنصر تمكين الناس، والناس بحاجة إلى المهارات والسلوك. فعناصر التمكين توفر المخرجات لصالح عناصر التمكين الأخرى (على سبيل المثال، العمليات توفر المعلومات والمهارات والسلوك). ولكل من هذه العناصر التمكينية السبعة التي عرفها كويت والموضحة في الشكل التوضيحي (٥-٦) خمسة مكونات نوعية هي:

١- أصحاب المصلحة لعنصر التمكين: على الرغم من أننا قد تحدثنا عن أهمية أصحاب المصالح باعتبارها عوامل محركة لعملية كويت بشكل كامل، فإن لكل عنصر من عناصر التمكين السبعة أصحاب المصلحة الداخليين والخارجيين الخاصين به^(*).

(*) الأطراف التي تلعب دوراً نشطاً و/ أو لديهم اهتمام بهذا العنصر (المترجم).

شكل توضيحي ٥-٦

أصناف أو أنواع عناصر التمكين في كويت



ف للعمليات أصحاب مصالح داخليين وخارجيين، ولكل منهم أدواره الخاصة، لذا يجب توثيق أصحاب المصلحة ومستويات مسؤولياتهم بطريقة تعبر عن سمات العملية.

٢- الأهداف والمقاييس المعيارية^(*): ينبغي تحديد أهداف عنصر التمكين على أنها بيان يصف النتيجة المأمولة من العملية. فقد تكون هذه النتيجة عبارة عن منتج صناعي Artifacts، أو تغييراً كبيراً على حالة العملية، أو تحسناً كبيراً في إمكانيات عمليات أخرى. وهي تمثل جزءاً من أهداف العملية التي تدعم الأهداف المتعلقة بتقنية المعلومات، والتي بدورها تدعم أهداف المؤسسة. في كل مستوى، يجب أن تقوم المقاييس المعيارية

(*) مؤشرات (المترجم).

بتعريف وقياس إلى أي مدى تم تحقيق هذه الأهداف. ويمكن تعريف المقاييس المعيارية على أنها كيانات قابلة للقياس الكمي وينبغي أن تكون محددة Specific، وقابلة للقياس Measurable، وقابلة للتنفيذ Actionable، وذات صلة Relevant، وضمن إطار زمني (محددة بوقت) Timely.

ويمكن تصنيف الأهداف بطرق مختلفة تتراوح بين الأهداف الاقتصادية، التي تعتبر أكثر توجهاً نحو تحقيق الكفاءة Efficiency، إلى أن تصل إلى أهداف الجودة، التي تعتبر أكثر توجهاً نحو تحقيق الفاعلية Effectiveness.

وبالمثل فإن هناك نوعين من مقاييس العملية: مقاييس الأداء التي لها طابع تنبؤي وهي تشير إلى مدى تنفيذ العملية للأنشطة المحددة، ومقاييس النتائج التي تشير إلى حجم أو مدى تحقيق العملية لأهدافها والغاية من وجودها.

٣. **دورة حياة عناصر التمكين:** لا بد من دعم كل من عناصر التمكين تلك بالخطط اللازمة لتأسيسه ومن ثم تأتي مراحل البناء والاستحواذ والإنشاء والتنفيذ له. وبعد استخدامها أو تشغيلها، فإن عناصر التمكين يجب أن تُراقب وتُقيّم بشكل دوري مع تحديث الهدف أو التخلص منها عند الضرورة.

٤. **الممارسات الجيدة:** لا بد من وضع وتحديد الممارسات الداخلية والخارجية باستخدام أدوات مثل الإطار كويت. فهناك مكونات داخلية وخارجية للممارسات الجيدة لعناصر التمكين، وكلاهما يشتمل على ممارسات جيدة في المهارات البشرية، متضمناً ذلك المتطلبات المهنية الموضوعية لكل دور من الأدوار التي يلعبها أصحاب المصالح المختلفين. ويمكن وصف ذلك من خلال التوصيفات الوظيفية المحددة لمستويات المهارات المختلفة باختلاف فئات أو أنواع المهارات. فأنواع أو فئات المهارات تعتمد على الأنشطة المرتبطة بتقنية المعلومات كإدارة شبكة الاتصالات أو تحليل الأعمال.

٥. **سمات عناصر التمكين:** لكل عنصر من عناصر التمكين هذه بعض السمات الفريدة التي تميزه عن غيره من العناصر التمكينية الأخرى الموجودة في المؤسسة.

"عنصر التمكين" هو مصطلح أو مفهوم لم يكن شائعاً في عمليات تشغيل وعمليات الأعمال قبل عدة سنوات. وقد اشتهر هذا المصطلح بداية من خلال الأوراق العلمية التي تتحدث عن قضايا تقنية المعلومات. وعلينا أن نتذكر أن عنصر التمكين هو أداة أو عملية توفر القدرات والكفاءات القابلة للقياس والتي من شأنها أن تحسن عمليات الأعمال، بدلاً من أن تقوم فقط بأتمتها. وهي عبارة عن قدرات وقوى وموارد تسهم في نجاح الكيان أو النشاط أو المشروع. إنها مفاهيم تستحق أن تضاف إلى قاموس مصطلحات أعمال المرء.

المبدأ الخامس لكوبت: هياكل قياس أداء الحوكمة والإدارة:

يركز المبدأ الرئيسي والأخير لكوبت على أهمية المفاهيم المختلفة إلا أنها مترابطة لكل من الإدارة والحوكمة في المؤسسة الموجهة نحو تقنية المعلومات. فقد ميز الإطار كوبت 5,0 بشكل واضح وجلي بين الحوكمة والإدارة. فكلاهما يتضمن أنواعاً مختلفة من الأنشطة ويتطلب هياكل تنظيمية مختلفة ويخدم أغراضاً مختلفة. فهذا التمييز يعد أساسياً بالنسبة لنظرة كوبت للحوكمة والإدارة.

إننا ننسى كثيراً أن الحوكمة governance، ذلك المصطلح الشائع في عالم الأعمال اليوم، مشتقة من الفعل اليوناني الذي يعنى "التوجيه" "to steer". حيث يشير نظام الحوكمة إلى كل الوسائل والآليات التي تمكن العديد من أصحاب المصلحة في المؤسسة من أن يكون لهم كلمة مؤثرة في تقييم الظروف والخيارات؛ تحديد الاتجاه؛ متابعة التوافق والأداء والتقدم المحرز مقابل الخطط الموضوعة لتلبية أهداف مؤسسية محددة. وكل هذا يشير إلى مجموعة كبيرة من الأنشطة التوجيهية. وتشتمل الوسائل والآليات هنا على أطر العمل والمبادئ والسياسات والرعاية والهياكل وآليات صنع القرار إلى جانب الأدوار والمسؤوليات والعمليات والممارسات اللازمة لتحديد الاتجاه ومتابعة الامتثال والأداء الذي يتسق مع الأهداف الشاملة. هذا هو التعريف الكبير والشامل نوعاً ما لحوكمة تقنية المعلومات، إلا أن الفصول التالية سوف تناقش القضايا الأخرى التي تدعم هذا التعريف. وعلينا أن نتذكر دائماً أنه في معظم المؤسسات، تكون الحوكمة مسؤولية مجلس الإدارة وتحت قيادة الرئيس التنفيذي CEO ورئيس مجلس الإدارة.

يتم غالباً تمييز الإدارة عن الحوكمة، فالإدارة تستلزم الاستخدام العادل للموارد والناس والعمليات والممارسات وغير ذلك لتحقيق الغاية المرجوة. فهي الوسيلة أو الأداة التي بها يحقق كيان (أو هيئة) الحوكمة نتيجة أو هدفاً. فالإدارة مسئولة عن التنفيذ ضمن الاتجاه الذي تم تحديده أو وضعه من قبل هيئة أو وحدة التوجيه. فالإدارة تتعلق بالتخطيط والبناء والتنظيم ومراقبة الأنشطة التشغيلية لتتماشى مع الاتجاه الموضوع من قبل هيئة الحوكمة.

تؤكد الإرشادات الخاصة بكويت أن الحوكمة والإدارة هما نوعان مختلفان من الأنشطة، ولكل منهما مسؤوليات مختلفة. ومع ذلك، وبالنظر إلى دور الحوكمة - في التقييم والتوجيه والمراقبة - فإن هناك مجموعة من التفاعلات المتبادلة المطلوبة بين الحوكمة والإدارة للحصول على نظام حوكمة ذي كفاءة وفاعلية. إذ يتم ربط هذه التفاعلات، باستخدام البنية المعمارية لعناصر التمكين، بعمليات محددة لمراجعة الضوابط الداخلية، التي تعد نقطة القوة الحقيقية لإطار العمل كويت.

مطابقة عمليات كويت مع أهداف تقنية المعلومات من خلال الجمع بينهما:

يحدد إطار العمل كويت ومواده الداعمة المنشورة مجموعة رفيعة المستوى من العمليات التي تحدد اتجاه أهداف أعمال المؤسسة وموارد تقنية المعلومات. وهي التي صُممت خصيصاً لتناسب إلى حد ما جميع أحجام المؤسسات وأنواعها، وقد تم تصنيف هذه العمليات إلى مجموعتين: الأولى باعتبارها عمليات لحوكمة تقنية المعلومات المؤسسية، والثانية هي مجموعة منفصلة من العمليات التي تقوم بتقديم الإرشادات الخاصة بإدارة تقنية المعلومات المؤسسية. تحتوي كل مجموعة من هاتين المجموعتين على سلسلة من الإجراءات أو العمليات الأكثر تفصيلاً. فبالنسبة لإدارة تقنية المعلومات في المؤسسة، هناك مجموعات من العمليات أو الإجراءات للقيام بالتالي:

- التوفيق والتخطيط والتنظيم.
- البناء والاستحواذ والتنفيذ.
- تقديم الخدمة والصيانة والدعم.
- التقييم والتوجيه والمتابعة.

كل مجموعة من هذه المجموعات تتضمن بعد ذلك عمليات أكثر تحديداً في كوبت. فبالنسبة لمجموعة البناء Build والاستحواذ Acquire والتنفيذ Implement فإن إرشادات كوبت تكون منظمة على شكل فئات لتحقيق أهداف الرقابة الداخلية باستخدام أسماء الترميز التالية المعرفة من قبل كوبت:

BAI1 - إدارة البرامج والمشروعات

BAI2 - تحديد المتطلبات

BAI3 - تعريف وبناء الحلول

BAI4 - إدارة الإتاحة والسعة

BAI5 - تمكين التغيير التنظيمي

BAI6 - إدارة التغييرات

BAI7 - قبول وانتقال التغييرات

BAI8 - إدارة المعرفة

وقد تم تعريف مجموعة مشابهة من فئات أهداف الرقابة الخاصة بالعملية لكل فئة من فئات العملية المذكورة. إن الغرض من عمليات الرقابة التفصيلية، وإن كانت محددة إلى حد ما، هو المساعدة في دراسة الحالة المؤسسية Business Case لتنفيذ وتحسين حوكمة وإدارة تقنية المعلومات. هدفها هو التعرف على كل نقطة من نقاط الألم أو النقاط الحرجة الأساسية والأحداث المحفزة، وذلك من خلال الهدف العام لخلق البيئة المناسبة لعمليات تشغيل تقنية المعلومات وتطبيقاتها.

لقد قام كوبت بتعريف مجموعة مكونة من ١٧ هدفاً مرتبطاً بتقنية المعلومات يمكن مناظرتها مع كل عملية من هذه العمليات. وتنقسم هذه الأهداف أيضاً إلى فئات أخرى معنونة بـ "الشركة" و"العميل" و"داخلياً" و"التعلم والنمو". وقد تتغير هذه العناوين عندما يتحول كوبت من مسودة النسخة النهائية الحالية، فئة مثل "الشركة" لا تعني أن الإرشادات تنطبق فقط على الشركات العامة، بل على المؤسسات بأكملها.

الشكل التوضيحي (V-0) يوضح المقابلة أو المناظرة بين أهداف كوبت المتعلقة بتقنية المعلومات والعوامل الخاصة بعمليتين من عمليات كوبت هما: (التقييم والتوجيه والمتابعة) (EDM) evaluate, direct, and monitor و(تقديم الخدمة والصيانة والدعم) (DSS) deliver, service, and support. فهذه المناظرة توضح كيف يتم دعم كل هدف من الأهداف المتعلقة بتقنية المعلومات من قبل إحدى عمليات كوبت. كما هو مبين بالشكل التوضيحي (V-0) والذي تم التعبير عنه باستخدام مقياس معين حيث إن:

- ر ترمز إلى علاقة رئيسية بين الهدف الخاص بتقنية المعلومات وعملية كوبت المرتبطة به، عندما تكون هناك علاقة هامة حيث تكون عملية كوبت المصممة داعماً رئيسياً لتحقيق هدف تقنية المعلومات.

- ث ترمز إلى ثانوي ذلك عندما لاتزال هناك علاقة أقل أهمية وتكون عملية كوبت داعماً ثانوياً لهدف تقنية المعلومات.

- فراغ عندما لا توجد في هذه الحالة علاقة قوية.

على سبيل المثال تمتلك عملية كوبت التي يرمز لها بالرمز DSS7 والخاصة بـ "إدارة الأمن" علاقة قوية أو رئيسية مع هدف تقنية المعلومات المدعو أو المسمى "الامتثال ودعم القوانين واللوائح التنظيمية" الخاصة بالمؤسسة. العملية DSS7 نفسها لها أيضاً علاقة ثانوية مع العديد من الأهداف الأخرى لتقنية المعلومات مثل الهدف رقم سبعة (V) والخاص بتقديم خدمات تقنية المعلومات وفقاً لمتطلبات الأعمال.

تؤكد إرشادات كوبت أن الحوكمة والإدارة هما نوعان مختلفان من الأنشطة، لكل منهما مسؤولياته المختلفة. ومع ذلك، ونظراً للدور التوجيهي الذي تلعبه الحوكمة - للتقييم والتوجيه والمتابعة - فإن هناك مجموعة من التفاعلات التبادلية الضرورية بين الحوكمة والإدارة للوصول إلى نظام حوكمة ذي كفاءة وفاعلية. ويتم بعد ذلك الربط بين هذه التفاعلات وعمليات محددة في كوبت خاصة بمراجعة الرقابة الداخلية، وذلك باستخدام البنية المعمارية لعناصر التمكين، وهو ما يعد القوة الحقيقية للإطار.

بالنسبة للعديد من كبار المديرين. قد يبدو إطار العمل كوبت أكثر تفصيلاً، وأنه يحتوي على مجموعة من الغايات والأهداف المعقدة بعض الشيء. ومن الممكن تحقيق الفائدة القصوى من استخدام كوبت فقط إذا تم تبنيه على نحو فعال وتكييفه ليلئم البيئة الفريدة لكل مؤسسة. فكل نهج تطبيقي سيكون أيضاً بحاجة إلى أن يُعالج تحديات محددة، بما في ذلك إدارة تغيرات الثقافة والسلوك. لقد لمس هذا الفصل فقط الهيكل العام لكوبت وإصداره الحالي (الإصدار الخامس).

شكل توضيحي (V-0)

مثال المقابلة بين أهداف الإطار كويت وأهداف تقنية المعلومات

		عمليات الإطار كويت	مجال أمن المعلومات					مجال أمن المعلومات								DSS8	
			مجال أمن المعلومات					مجال أمن المعلومات									
			EDM1	EDM2	EDM3	EDM4	EDM5	DSS1	DSS2	DSS3	DSS4	DSS5	DSS6	DSS7	DSS8		
			فهم بوضوح وصيانة إطار عمل الحوكمة	تأكد من تعميم القيمة	تأكد من تعميم المخاطر	تأكد من تعميم الموارد	تأكد من شمولية أصحاب المصلحة	فهم إدارة عمليات التشغيل	فهم إدارة العمليات	فهم إدارة الهوية	فهم إدارة طلبات وحالات الخدمة	فهم إدارة المشاكل	فهم إدارة الاستمرارية	فهم إدارة الأمن	فهم إدارة صوابية عمليات الأعمال		
الأهداف المتعلقة بتقنية المعلومات	1	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓	✓	✓	✓	✓						✓	✓			
	2	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓		✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	
	3	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓	✓	✓	✓	✓										
	4	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓		✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	
	5	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓	✓		✓		✓	✓			✓	✓				
	6	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓	✓	✓	✓	✓										
	7	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	
	8	تطوير وتنفيذ وإدارة إطار عمل الحوكمة		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	
	9	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓			✓		✓	✓	✓		✓	✓				
	10	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓		✓			✓		✓	✓			✓	✓	✓	
	11	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓	✓		✓		✓				✓	✓				
	12	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓	✓					✓			✓				✓	
	13	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓	✓	✓	✓	✓		✓			✓		✓			
	14	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓	✓	✓		✓	✓		✓		✓	✓	✓	✓	✓	
	15	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓		✓		✓	✓	✓				✓	✓		✓	
	16	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓	✓	✓	✓			✓		✓		✓			✓	
	17	تطوير وتنفيذ وإدارة إطار عمل الحوكمة	✓	✓	✓	✓	✓						✓	✓		✓	

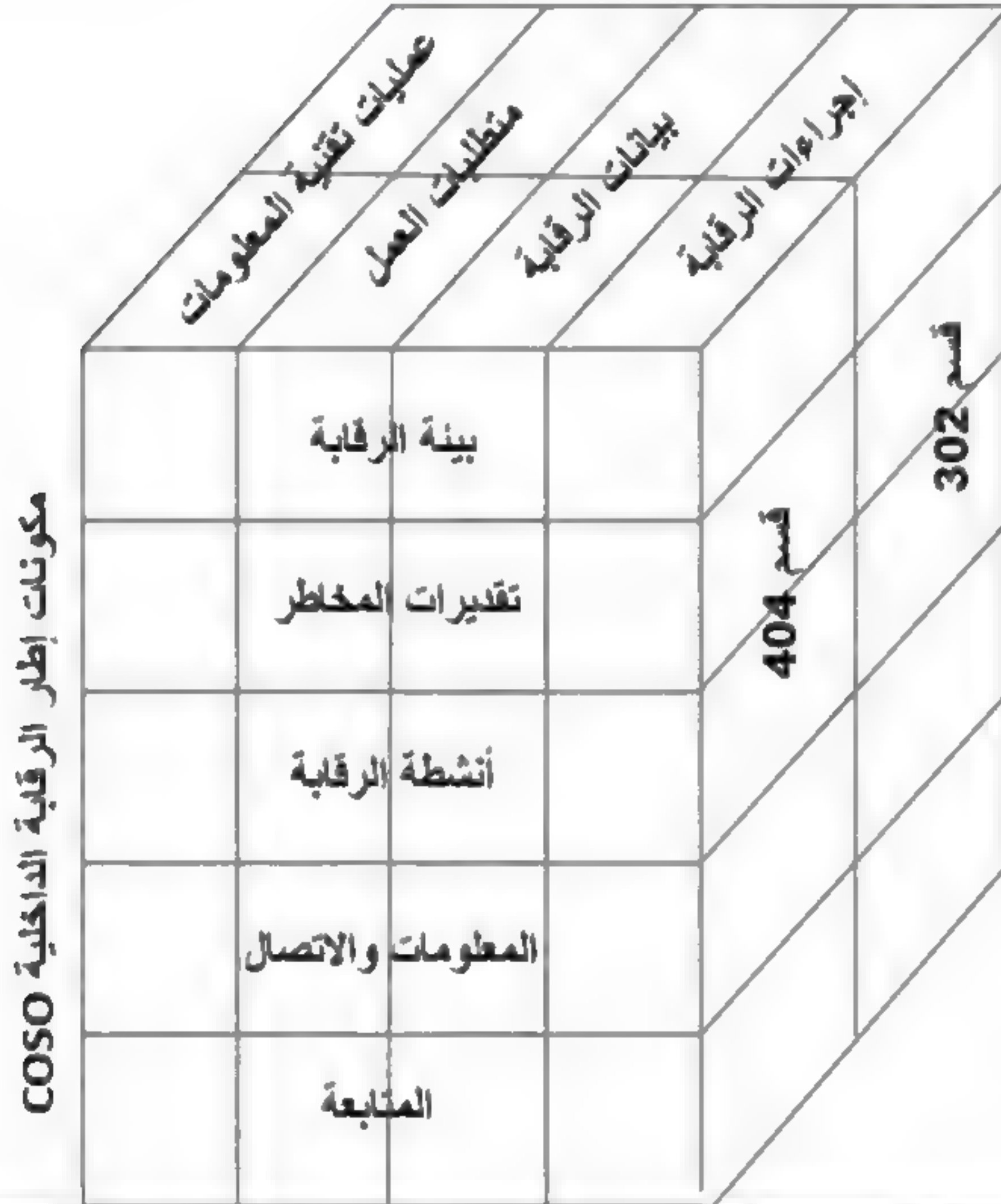
استخدام كوبت في بيئة قانون ساربنز أوكسلي (SOx):

عندما تم تفعيل قانون ساربنز أوكسلي SOx للمرة الأولى في الولايات المتحدة، كان هناك القليل من الإرشادات حول كيفية تطبيق وإدارة البند ٤٠٤ من هذا القانون والخاصة بمراجعات الرقابة الداخلية. وقد أشار مجلس الإشراف المحاسبي على الشركات المساهمة Public Company Accounting Oversight Board (PCAOB)، الذي تقدم عرضه في الفصل الثاني من هذا الكتاب، إلى أنه كانت لديه النية لوضع بعض المعايير المحددة، إلا أنه قد تعمد في البداية ترك المؤسسات والمدققين الخارجيين دون توجيه. ومع التشديد المكثف على أنظمة الرقابة الداخلية الرفيعة المستوى لتقنية المعلومات، قامت العديد من المؤسسات بتبني الإطار باعتباره إطاراً خاصاً بالرقابة الداخلية على أنه أحد الخيارات التي تساعد في تحقيق الامتثال لقانون ساربنز أوكسلي SOx.

قام البند ٤٠٤ من قانون ساربنز أوكسلي SOx الخاص بمتطلبات تقييم الرقابة الداخلية بتسليط الضوء على النهج القائم على المخاطر لتقييم الضوابط الداخلية مع التأكيد على إطار الرقابة الداخلية COSO، الذي تم الحديث عنه في الفصل الرابع من هذا الكتاب. يعد كوبت بمثابة إطار عمل بديل وقوي لتقييم الضوابط الداخلية ولاسيما في البيئات التي تركز بشكل مكثف على عمليات وموارد تقنية المعلومات. ويمكن وصف كل من الرقابة الداخلية الخاصة بلجنة المنظمات الراعية (COSO) وكوبت على أنها أطر عمل متعددة الأبعاد لوصف بيئات الرقابة الداخلية الخاصة بكلٍ منهما. فكل منهما يشبه الآخر ولكن مع وجود اختلافات طفيفة في التصنيفات والمصطلحات. الشكل التوضيحي (٨-٥) يبين المناظرة أو المقابلة بين الإطار كوبت ونموذج الرقابة الداخلية (COSO).

شكل توضيحي (٨-٥)

العلاقة بين مكونات COSO وأهداف COBIT
أهداف COBIT



يمكن استخدام أهداف كوبت، بدءاً من التخطيط والبدء في تنفيذ المشاريع وصولاً إلى المتابعة والتقييم لفهم وتقييم الضوابط الداخلية من خلال المكونات الخمسة لإطار الرقابة الداخلية COSO. وسواء تم استخدام إطار الرقابة الداخلية COSO بشكل عام أم تم استخدام كوبت، فإن تحليل هذين الإطارين اللذين ينطلق من خلالهما سلسلة من العمليات تبدأ من التخطيط إلى إجراء تقييمات المخاطر، حتى نصل إلى تحديد وتوثيق

وتقييم الضوابط الداخلية الرئيسية؛ كل ذلك سيساعد المؤسسة على تحقيق الامتثال للبند ٤٠٤ من قانون ساربنز أوكسلي SOx. أضف إلى ذلك، أنه من خلال الدعم المقدم لكوبت من قبل المنظمة المهنية ITGI والقبول الدولي الواسع النطاق له، يعد وثيقة حية يتم تحديثها من وقت لآخر.

في ظل وجود قانون ساربنز أوكسلي SOx، والتشديد المتزايد على حوكمة تقنية المعلومات، وإدراك مدى أهمية تقنية المعلومات في معظم قرارات الرقابة الداخلية، فقد مر كوبت بعدة مراجعات حتى وصل إلى نسخته الحالية الممثلة بالإصدار الخامس الذي سيتم إطلاقه قريباً. لقد قام معهد حوكمة تقنية المعلومات الراعي لكوبت بعمل رائع هو إصدار مجموعة من المطبوعات التي ترسم علاقة الإطار كوبت مع تلك المعايير الأخرى.

إن المجموعة الكاملة من مواد أهداف الرقابة في كوبت سوف توفر دعماً قوياً لفريق الإدارة الذي يقوم بإجراء مراجعة لتقييم الرقابة الداخلية في ضوء البند ٤٠٤ من قانون SOx. وعلى الرغم من أنه يمكن استخدام هذه المفاهيم في أي مجال من مجالات الرقابة الداخلية، فإن التركيز هنا فقط على تطبيقات وعمليات تقنية المعلومات. وبالنسبة للعديد من المؤسسات فإن فهم وتقييم الرقابة الداخلية المرتبطة بتقنية المعلومات هو المفتاح لتحقيق الامتثال لقانون SOx. وعلى الرغم من أن كوبت موجود منذ سنوات عديدة فإنه ولفترة طويلة كان الكثير ينظر إليه على أنه مجرد أداة متخصصة لتدقيق تقنية المعلومات، ولم يكن يُنظر إليه على أنه يقدم المزيد من المساعدة في أعمال التقييم الأخرى للضوابط الداخلية والتدقيق الداخلي بوجه عام. وعلى الرغم من أن تركيز كوبت لا يزال مُنصباً على تقنية المعلومات، فإنه يجب على كبار المديرين أن يقوموا باستكشاف هذا الإطار باعتباره أداة ممتازة للمساعدة في الامتثال للمتطلبات الحالية والمتطورة لقانون SOx.

كوبت في دائرة الضوء:

ينبغي على جميع كبار المديرين المتخصصين سواء في التشغيل أم في المالية أو تقنية المعلومات في المؤسسة أن يكون لديهم على الأقل فهم عالي المستوى لإطار العمل كوبت. فهو بوجه خاص أداة مفيدة وهامة لتقييم نظم الرقابة المالية الداخلية والعمليات الشاملة للحوكمة في بيئة أكثر توجهاً نحو تقنية المعلومات — وهي البيئة التي نواجهها تقريباً اليوم

بشكل دائم. إن قرار استخدام كوبت في عمليات حوكمة تقنية المعلومات لا ينبغي أن يكون مؤقتاً أو قراراً فردياً لأحد كبار المديرين. بل ينبغي على كبار المديرين وكذلك المتخصصين في الرقابة الداخلية والمدققين الداخليين لديهم في المؤسسة القيام بتطوير الأهداف واتخاذ الخطوات اللازمة لتنفيذ إطار العمل كوبت.

يعد كوبت إطار للرقابة الداخلية وأداة تقييم رائعة - وفي بعض الأحيان رائعة للغاية - لوضع عمليات خاصة بحوكمة تقنية المعلومات وتقييم الضوابط الداخلية لها. ولعل أكبر عائق يواجهه الإدارة العليا التي تحاول استخدام كوبت بشكل كامل هو أن هذا الإطار قد تم بناؤه في الأصل ليكون بالمقام الأول أداة لتدقيق تقنية المعلومات. على الرغم من أن انتقال رعاية المواد الإرشادية لكوبت من إزاكا إلى ITGI قد أدى إلى توسيع جاذبيتها وتركيزها، فإن هناك تركيزاً كثيفاً جداً على تقنية المعلومات في العديد من هذه المواد المنشورة. ومن المؤكد أن هذا يخيف البعض.

تكمّن القوة الحقيقية لكوبت في تركيزه على حوكمة تقنية المعلومات كما هو مبين في الشكل التوضيحي (٥-١). حيث يوضح الشكل أهمية التحالف الإستراتيجي بين الأعمال وموارد تقنية المعلومات إلى جانب إيصال القيمة وإدارة الموارد وإدارة المخاطر وعمليات قياس الأداء. وهذه الأمور تسمح للمؤسسة بتأسيس حوكمة فعالة لتقنية المعلومات، وينبغي أن يساعد كوبت في إدارة وفهم هذه المفاهيم. ولنا أن نتوقع استمرار نمو المعايير والممارسات المنشورة لكوبت والذهاب إلى ما هو أبعد من كونها مجرد مفاهيم أساسية خاصة بـ "تدقيق تقنية المعلومات".

ملاحظات:

- ١- يقع كلٌّ من معهد حوكمة تقنية المعلومات (ITGI) وجمعية ضبط وتدقيق نظم المعلومات (ISACA) في مدينة رولينج ميدوز بولاية إلينوي الأمريكية.
- ٢- كوبت ٥: المسودة الخاصة بعرض الإطار (رولينج ميدوز، إلينوي، معهد حوكمة تقنية المعلومات، ٢٠١١).

الفصل السادس

إرشادات إطار آيتيل (ITIL) وإدارة خدمات تقنية المعلومات

في الواقع لم يكن مفهوم إدارة خدمات تقنية المعلومات IT SERVICE MANAGEMENT (ITSM) معروفاً في الأيام الأولى لإدارات عمليات تشغيل تقنية المعلومات الخاصة بمؤسسات الأعمال. فإدارة خدمات تقنية المعلومات ITSM عبارة عن النظام أو الأسلوب المتبع لإدارة نظم تقنية المعلومات التي تعتمد على رأي العميل في حجم مساهمة تقنية المعلومات في الأعمال. تعمل عمليات إدارة خدمات تقنية المعلومات بشكل مدروس ومرتزن على عكس الأساليب التقنية المركزية التي كانت تستخدم في الماضي لإدارة تقنية المعلومات، وتعد العمليات القوية لإدارة خدمات تقنية المعلومات من العناصر الهامة في الحوكمة الفعالة لتقنية المعلومات.

يستعرض هذا الفصل القضايا الهامة في إدارة خدمات تقنية المعلومات ITSM بالنسبة للحوكمة الفعالة لتقنية المعلومات، وذلك من خلال تعريف كبار محترفي الأعمال المتخصصين لمكتبة البنية التحتية لتقنية المعلومات Information Technology Infrastructure Library (ITIL)، وهي عبارة عن مجموعة من أفضل الممارسات المتعارف عليها دولياً والتي تغطي معظم الجوانب الخاصة بعمليات تشغيل تقنية المعلومات.

آيتيل (ITIL) هو اختصار متعارف عليه ومُعترف به للمواد الإرشادية الآخذة في التوسع والتي وُضعت لأول مرة في ثمانينيات القرن الماضي من قبل مكتب التجارة الحكومية (Office of Government Commerce (OGC) التابع للحكومة البريطانية. وعلى الرغم من أنها كانت في الأصل عبارة عن مكتبة كتب حقيقية، فإنها اليوم تعد مجموعة من أفضل الممارسات المستقلة لتقنية المعلومات والتي يتم تحديثها بانتظام والتي قد تم اعتمادها في البداية على نطاق واسع من قبل عمليات تشغيل تقنية المعلومات في المملكة المتحدة، ثم تلاها بعد ذلك الاتحاد الأوروبي (European Union (EU، وقد شاع استخدامها الآن بشكل متزايد في الولايات المتحدة الأمريكية. وكما هو الحال تماماً بالنسبة لشركة آي بي إم (IBM) التي أصبحت اسماً بحد ذاتها بدلاً من كونها اختصاراً لآلات

الأعمال العالمية International Business Machines، فإن معظم المهنيين المحترفين هذه الأيام قد نسوا الكلمات التي يتكون منها ITIL.

آيتل (ITIL) عبارة عن إطار عمل تفصيلي لأفضل الممارسات المهمة لتقنية المعلومات، بما فيه من قوائم مراجعة ومهام وإجراءات ومسؤوليات شاملة تم تصميمها لتتلاءم مع أي إدارة من إدارات تقنية المعلومات. فمن خلال تقسيم العمليات الأساسية الخاصة بتقديم الخدمات إلى عمليات خاصة بتقديم خدمات تقنية المعلومات وعمليات تعمل على دعم الخدمات؛ أصبح آيتل الآن في واقع الأمر أسلوباً أو منهجية لوصف العديد من العمليات الأساسية الموجودة في إدارة خدمات تقنية المعلومات، مثل إدارة التهيئة أو إدارة التغيير. ويحدد إطار آيتل سلسلة من أفضل الممارسات الأساسية التي لا غنى عنها في حوكمة تقنية المعلومات.

تعد مفاهيم آيتل هامة بالنسبة للحوكمة الفعالة للعمليات التشغيلية في تقنية المعلومات في أي مؤسسة. وبشكل مغاير تماماً للأيام الأولى لظهور نظم تقنية المعلومات المؤسسية عندما كان يقوم مطورو نظم وإدارات تشغيل تقنية المعلومات ببناء العديد من النظم الرئيسية المرتبطة بتقنية المعلومات، فإن إدارة خدمات تقنية المعلومات (ITSM) تدعو مستخدمي تلك التقنية إلى أن يكون لهم دور أكبر بكثير في مثل هذه العمليات الشاملة.

أساسيات آيتل:

آيتل عبارة عن (أو كان في وقت من الأوقات) "مكتبة" رسمية للمطبوعات التقنية، التي نشرت من قبل مكتب تجارة الحكومة البريطاني^(١) British Office of Government Commerce. حيث يتم التحكم في المطبوعات ومحتوياتها بشكل محكم، وذلك على غرار مطبوعات المعايير الدولية الصادرة عن الأيزو ISO، والتي تم الحديث عنها في الفصل السابع من هذا الكتاب. يقدم آيتل إطار عمل لحوكمة تقنية المعلومات يركز على القياس والتحسين المستمر لجودة خدمات تقنية المعلومات المقدمة، وذلك من منظور الأعمال والعملاء. وقد كان لهذا التركيز دور رئيسي في نجاح آيتل في جميع أنحاء العالم، كما أسهم أيضاً في استخدامه وفي الفوائد

الرئيسية التي حصلت عليها المؤسسات التي قامت بنشر تقنيات وعمليات آيتل في جميع أنحاء الإدارات التابعة لهم. وفيما يلي بعض من هذه الفوائد:

- تزايد رضا المستخدم والعميل عن خدمات تقنية المعلومات التي يتم تقديمها.
- تحسين إتاحة الخدمات يؤدي بشكل مباشر إلى تزايد محتمل لأرباح وعائدات الأعمال.
- تحقيق توفيرات مالية نتيجة تقليل تكرار العمل وتقليل الوقت المهدر وتحسين إدارة الموارد واستخدامها.
- تحسين الوقت لتسويق النواحي الخاصة بتقنية المعلومات من منتجات وخدمات جديدة.
- تحسين صنع القرار وتحسين المخاطر لكافة العمليات ذات الصلة بتقنية المعلومات.

تشمل أفضل ممارسات آيتل الخاصة بتقديم الخدمات ما يطلق عليه غالباً مصطلح البنية التحتية لتقنية المعلومات، وهي العمليات الداعمة التي تسمح لتطبيقات تقنية المعلومات بالعمل وتوصيل نتائجها لمستخدمي النظم. في كثير من الأحيان، كانت إدارة المؤسسة تركز اهتماماتها على الجانب التطويري للتطبيقات المرتبطة بعمليات تقنية المعلومات وتهمل الدعم الهام والضروري لعمليات تقديم الخدمات. فمن الممكن على سبيل المثال أن تبذل المؤسسة مجهوداً ضخماً في بناء وتطبيق نظام جديد للتنبؤ بالميزانية، غير أن القيمة الحقيقية المكتسبة من هذا التطبيق أو النظام الخاص بالميزانية ستكون قليلة ما لم تكن هناك عمليات وإجراءات جيدة معمول بها وموضوعة في موضع التنفيذ، كعمليات إدارة المشاكل والحوادث، التي تسمح لمستخدمي هذا النظام (التنبؤ بالميزانية) بأن يقوموا بالإبلاغ عن الصعوبات أو المشاكل التي تواجههم أثناء استخدامهم له. ومن الضروري أيضاً أن تكون هناك عمليات جيدة تتعلق بالسعة والإتاحة لكي تسمح للتطبيق الجديد بالعمل بالشكل المطلوب. إن جميع عمليات الآيتل هذه تعد جزءاً من البنية التحتية لتقنية المعلومات، فالتطبيقات المحكّمة والمصممة على نحو جيد تكون قيمتها محدودة بالنسبة لمن يستخدمها في حال عدم وجود مثل هذه العمليات القوية الخاصة بدعم وتقديم الخدمة في موضعها الصحيح.

في الوقت الذي انتشرت فيه أفضل الممارسات آيتل خلال السنوات الأخيرة في العديد من الأماكن الأخرى في العالم، أصبحت الآن أيضاً أكثر قبولاً ومعتزفاً بها على نطاق واسع داخل الولايات المتحدة. تقدم الأجزاء التالية لكبار المديرين نظرة عامة عن العمليات الهامة والخاصة بتقديم الخدمات في آيتل. وهذا من شأنه أن يقدم بعض الإرشادات المتعلقة بالكيفية التي يجب من خلالها أن تمتلك إدارات تقنية المعلومات في المؤسسة عمليات فعالة وفي الموضع المناسب لها، مثل وجود مكتب مساعدة أو خدمة العملاء، في المجالات المهمة لعمليات تقنية المعلومات. لا يحدد آيتل معايير بعينها لبناء وإدارة الضوابط الخاصة بتقنية المعلومات، ولكنه يقترح طرقاً جديدة لتنفيذ وتشغيل ضوابط عامة للبنية التحتية التي ينبغي أن يكون معمولاً بها بالفعل.

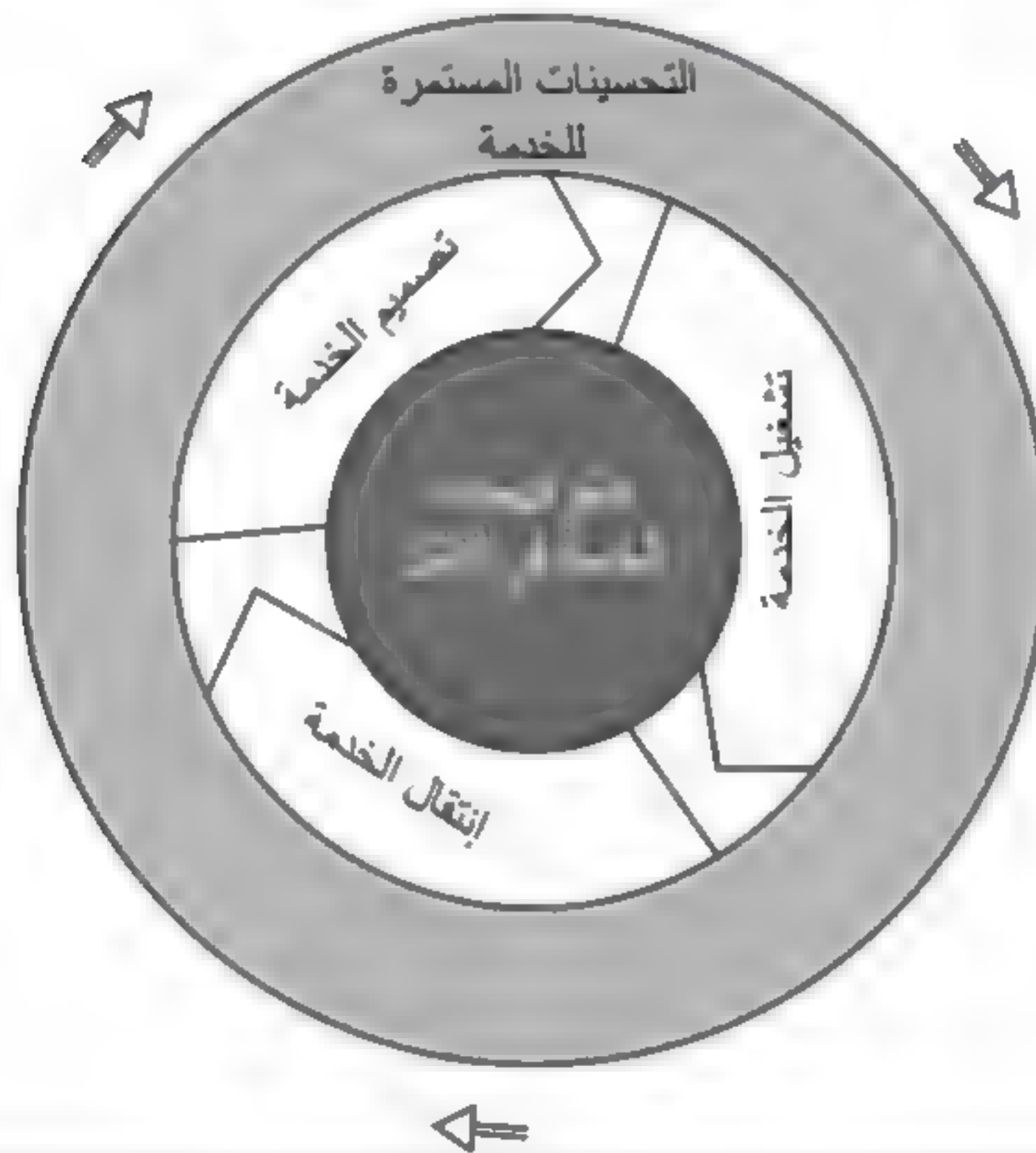
يمكن النظر إلى إستراتيجيات تقديم الخدمة الموجودة في آيتل على أنها دورة مستمرة لحياة النشاط، حيث تحتوي هذه العملية على ثلاث أنشطة تم عرضها في الشكل التوضيحي (٦-١) وهي: تقديم الخدمة ودعم الخدمة وانتقال الخدمة. وسنقوم بمناقشة كل من هذه الأنشطة في الأجزاء التالية. إن المبدأ الرئيسي هنا هو أن المؤسسة المستعدة لتطبيق الآيتل ينبغي أن يكون لديها عمليات مستمرة وجاهزة تتعلق بالخدمات وتتضمن جميع العمليات الأخرى في إدارة الخدمات وتستقبل مدخلات من مصادر خارجية لعملاء تقنية المعلومات. تقع العملية الخاصة بإستراتيجية الخدمة في وسط هذه الحلقات المركزية. حيث تشتمل هذه العملية الأساسية أو المركزية على السياسات والممارسات الخاصة بإدارة تقنية المعلومات والتي تم وصفها في عنصر بيئة الرقابة في إطار الرقابة الداخلية (COSO) والذي تم طرحه في الفصل الرابع من هذا الكتاب. كما يُظهر الشكل التوضيحي (٦-٢) هذا النموذج نفسه الخاص بتقديم الخدمات كعملية لخريطة سير التغذية الراجعة.

وقد جرت العادة على تقسيم عمليات آيتل إلى عمليات لدعم الخدمات وعمليات لتقديم الخدمات. فعمليات دعم الخدمة تساعد في جعل تطبيقات تقنية المعلومات تعمل بطريقة فعالة ومرضية للعميل، في حين تعمل عمليات تقديم الخدمة على تحسين كفاءة وأداء عناصر البنية التحتية لتقنية المعلومات. وهناك خمس عمليات لأفضل الممارسات المتعلقة بدعم الخدمات في آيتل والتي تبدأ بالعملية التي يطلق عليها إدارة

الإطلاق Release Management ، وهي المعنية بوضع منتج تقنية المعلومات في البيئة الإنتاجية، إلى أن تصل إلى عملية إدارة الحوادث Incident Management ، وهي المعنية بعمليات الإبلاغ المنتظم عن المشاكل أو الحوادث الموجودة في تقنية المعلومات. تشتمل عمليات دعم الخدمة في آيتل على الممارسات الجيدة أو الرشيدة لأي إدارة من إدارات تقنية معلومات مؤسسية، والتي تمتد من عملية التشغيل المركزي القائمة على استخدام الخادم أو النظم التقليدية القديمة للحاسبات المركزية كنقطة تحكم مركزية لتقنية المعلومات الخاصة بها إلى أن تصل إلى العمليات التشغيلية المنتشرة بكثرة لنظم (الخادم - العميل).

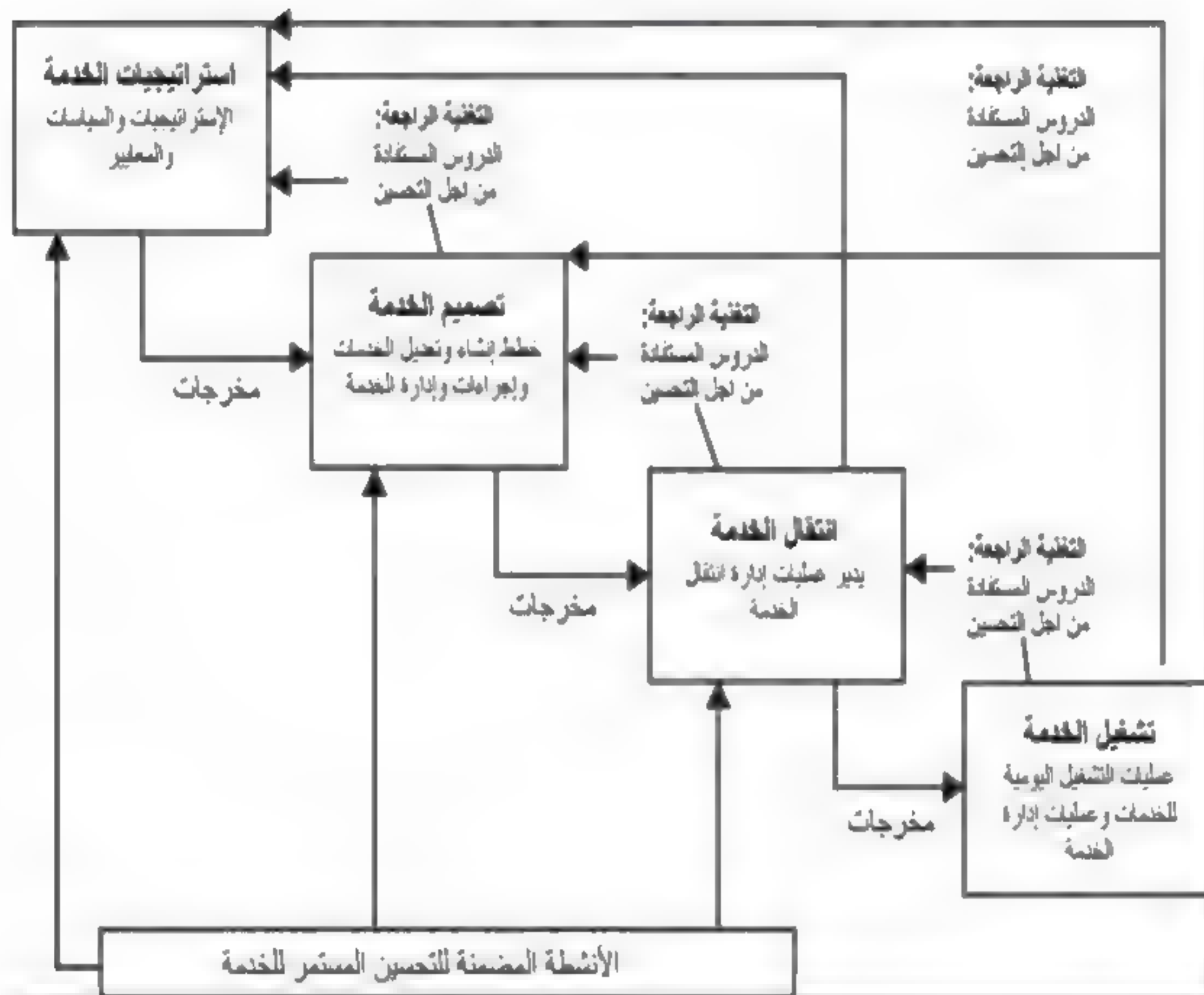
شكل توضيحي (١-٦)

دورة التغذية الراجعة المستمرة في آيتل



شكل توضيحي (٢-٦)

عمليات التغذية الراجعة للخدمة في الأيتل



ونظراً لوجود العديد من الاختلافات المحتملة في إدارة العمليات التشغيلية لتقنية المعلومات، فإن آيتل لم يحدد التفاصيل المتعلقة بـ "كيف" يتم تطبيق عمليات دعم الخدمة مثل إدارة التهيئة أو إدارة التغيير. وإنما يقوم آيتل باقتراح مجموعة من الممارسات والطرق الجيدة لإدارة المدخلات والعلاقات بين تلك العمليات. ولا يوجد أي ترتيب أو أسبقية لأي من هذه الممارسات والطرق. فمن الممكن النظر إليها وإدارتها بشكل منفصل، ولكنها جميعاً ترتبط بطريقة ما بعضها مع بعض. تقدم مجالات إدارة الخدمة الخاصة بتقديم ودعم الخدمة المتاحة في آيتل إلى جانب إدارة أمن المعلومات، الربط بين العمليات التشغيلية للأعمال وإدارة تقنية المعلومات والسنة التحتية الخاصة بها.

وعلى الرغم من أن هناك العديد من العناصر المستقلة لكنها مترابطة مع آيتل، فإن هذا الفصل سيناقش فقط مكونات دورة حياة الخدمة في آيتل والتي تعد أكثر أهمية بالنسبة للعمليات الفعالة لحوكمة تقنية المعلومات. تقترح أفضل الممارسات في آيتل أساليب مفضلة للعمليات التشغيلية لتقنية المعلومات لتشغيل النظم الإنتاجية لتقنية المعلومات بطريقة تسمح بتعزيز كفاءة العمليات وتقديم خدمات ذات جودة عالية لعملاء أو مستخدمي الخدمات. وتكون هذه الأساليب مفيدة على وجه الخصوص عند إجراء عملية التقييم وتقديم التوصيات في إحدى مجالات العمليات التشغيلية لتقنية المعلومات.

أثناء القيام بمراقبة ومراجعة الضوابط الداخلية لعمليات تشغيل تقنية المعلومات، فإن أحد الطرق التي تكون غالباً مجدية هو التفكير في مجال تقنية المعلومات الذي يجري مراجعته من حيث عمليات الإطار آيتل المستقلة والمذكورة في الأجزاء التالية. على سبيل المثال، فإن إحدى عمليات آيتل التي تسمى إدارة الحوادث، أو التي يطلق عليها عادة "مكتب المساعدة"، هي إحدى الخدمات المساندة أو الوسيلة التي يمكن استخدامها من قبل عملاء ومستخدمي النظم في حال وجود أي استفسار أو مشاكل حول العمليات التشغيلية لتقنية المعلومات. وعلى الرغم من الأهمية القصوى للإدارة الخاصة بمكتب المساعدة، فإنه يكون غالباً مصدر شكوى، مثال على ذلك، طرح المشكلة نفسها عدة مرات دون وجود أي جهود مبذولة بشكل واضح لتحليل الأمور والشروع في حلها. وبالنظر إليه على أنه ليس مجرد كونه مكتب مساعدة تقليدياً، بل على أنه عملية شاملة يتم من خلالها تحويل المسائل إلى عمليات الدعم الأخرى؛ فإن ذلك سوف يحسن أداء وجودة جميع العمليات التشغيلية المتعلقة بتقنية المعلومات في هذه الحالة.

عناصر إستراتيجية الخدمة في آيتل:

يبين الركن العلوي الأيسر من الشكل التوضيحي (٦-٢) الذي يعرض الرسم التخطيطي لعمليات حلقة التغذية الراجعة في آيتل، وظيفة تسمى إستراتيجيات الخدمة. يصف هذا العنصر سياسات وإستراتيجيات ومعايير إدارة الخدمة في آيتل، ويقوم أيضاً بتقديم المدخلات والإرشادات اللازمة للعمليات الأخرى في آيتل وهي تصميم ونقل وتشغيل الخدمة. كما ستقوم تلك العمليات الثلاثة الأخيرة لاحقاً بتقديم المدخلات الضرورية لعملية إستراتيجيات الخدمة لإجراء التحسينات المستمرة عليها.

وكواحدة من أفضل الممارسات الخاصة بحوكمة تقنية المعلومات، يقترح آيتل أن يقوم القائمون على إدارة تقنية المعلومات أولاً بتقييم إستراتيجية الخدمة الخاصة بهم، وذلك من خلال قيامهم بتوجيه بعض الأسئلة الجادة لأنفسهم والتي تتعلق بجودة خدمة تقنية المعلومات التي يقدمونها والتي تشمل:

- أي من خدمات تقنية المعلومات التي نقدمها أو عروض الخدمة هي الأكثر تميزاً؟
- أي من الخدمات التي نقدمها هي الأكثر ربحية للمؤسسة بأكملها؟
- أي من عملائنا وأصحاب المصلحة هم الأكثر رضا؟
- ما المجالات أو الخدمات التي قد تكون نقاط مشاكل محتملة أو مجالات لعدم الرضا؟
- أي من الأنشطة التي نقوم بها هي الأكثر اختلافاً وفاعلية؟

هذه الأسئلة ليست من النوعية التي تقوم إدارة تقنية المعلومات عادة بتوجيهها، سواء من الإدارة أثناء قيامها بتقييم موارد تقنية المعلومات لديها أو من قبل الإدارة العليا أو المدققين الداخليين. بل تمثل بعض الأسئلة الهامة التي ينبغي أن تؤخذ بالحسبان من قبل إدارة تقنية المعلومات أثناء قيامها بتقييم إستراتيجيات خدمات تقنية المعلومات التي تقدمها. والفكرة هي تحفيز إدارة تقنية المعلومات في المؤسسة لكي تكون أكثر من مجرد مصدر للحفاظ على عمليات تقنية المعلومات، بل لتكون أحد المصادر التي تقدم خدمات ذات قيمة عالية للمؤسسة بالكامل وبتكلفة معقولة. الشكل التوضيحي (٦-٣) عبارة عن قائمة لبعض الأسئلة الأخرى التي تساعد إدارة تقنية المعلومات للنظر في قدراتها وعروضها الإستراتيجية وتحسينها.

ستكون هناك حاجة لاتباع النهج المتعدد التخصصات للقيام بالرد على هذه الأسئلة المطروحة في الشكل التوضيحي (٦-٣)، وذلك بسبب اقتراح آيتل الذي ينص على أنه ينبغي على إدارة تقنية المعلومات أن تتعامل مع العديد من الإدارات كالعمليات التشغيلية، والمالية، وإدارة الجودة، والتدقيق الداخلي لتتمكن من فهم وتحديد الإستراتيجيات الرئيسية لتقنية المعلومات في المؤسسة بشكل أفضل. الفكرة كلها هي أنه يجب على قسم أو مجموعة تقنية المعلومات أن يقرروا ما هو وضعهم بالنسبة لكامل المؤسسة،

وما الخدمات التي بإمكانهم أن يقدموها. فقد ينتج عن هذا الأمر الدليل أو البيان الخاص بمحفظه الخدمات والذي يقوم بتحديد القدرات وعروض الخدمات الخاصة بتقنية المعلومات.

تحدث الفصل الخامس من هذا الكتاب عن استخدام إطار العمل كوبت في وضع ضوابط عامة وفعالة لتقنية المعلومات؛ فهذه الأنواع المقنعة من الضوابط العامة قد استخدمت في جميع العمليات التشغيلية لتقنية المعلومات في المؤسسة لتوفير الحماية الكافية لجميع النظم والتطبيقات. ومن الممكن أن تكون الأقفال المادية والضوابط الأمنية الأخرى لمركز الخوادم أو النظام الشائع لأمن تقنية المعلومات القائم على استخدام كلمات المرور والذي يغطي جميع العمليات التشغيلية لتقنية المعلومات في المؤسسة، أمثلة على تلك الضوابط العامة. وكما أكد الفصل الرابع على الضوابط الداخلية (COSO)، وكذلك الفصل الخامس، فإن سوء تنفيذ نظم الرقابة الداخلية لتقنية المعلومات أو ضعفها سوف يؤثر في جميع تطبيقات تقنية المعلومات والتي تعد جزءاً من تلك العمليات التشغيلية لنظم تقنية المعلومات.

في ظل ما يشهده العالم اليوم من الانتشار الواسع لعمليات ونظم تقنية المعلومات الموجودة في جميع أنحاء المؤسسة والتي تمتد من التطبيق الخاص بالتحكم في إحدى عمليات وحدات الأعمال ووصولاً إلى شبكة الإنترنت واسعة الانتشار، فإنه ينبغي أن يكون لدى كل من إدارة المؤسسة والموظفين المعنيين فهم جيد للتقنيات المستخدمة للرقابة الداخلية في تقنية المعلومات. وعلى الرغم من صعوبة تحديد الخطوط الفاصلة في بعض الأحيان، إلا أننا نستطيع التفكير بشكل عام في ضوابط تقنية المعلومات على مستويين عريضين هما: ضوابط التطبيقات التي تغطي عملية بعينها (مثل تطبيق مدفوعات الحسابات لدفع فواتير المشتريات)، وما يطلق عليه ضوابط عامة لتقنية المعلومات. وتشتمل هذه الفئة الأخيرة من الضوابط على العديد من الضوابط التي تتجاوز تلك التي ناقشناها في الفصل الرابع من هذا الكتاب، غير أنها مهمة لجميع جوانب العمليات التشغيلية الخاصة بتقنية المعلومات المؤسسية.

شكل التوضيحي (٦-٣)

أسئلة لتنمية القدرات الإستراتيجية في آيتل

- ما خدمات تقنية المعلومات التي ينبغي أن نقدمها؟ ولمن؟ بمعنى، هل نخدم جميع وحدات المؤسسة أو عينة محدودة أو عملاء من الخارج؟
- كيف نميز أنفسنا عن البدائل المنافسة؟ قد يقدم مزودو الخدمات الخارجيين خدمات بديلة، ولكن ما التكاليف أو القيم الفريدة التي تجعل إدارة تقنية المعلومات تظهر كبديل أفضل؟
- هل لدى فريق الإدارة إدارات أخرى بديلة لتقديم خدمات تقنية المعلومات من خارج المؤسسة يمكن أخذها في الاعتبار بجدية؟
- كيف يمكننا حقاً خلق قيمة لعملائنا؟ في كثير من الأحيان، تعالج تقنية المعلومات فقط الخدمات المطلوبة مثل تقارير الإقفال المالي في نهاية الشهر ولكن لا تعالج المعلومات اللازمة لاتخاذ قرارات تخص الاستجابة السريعة. لذلك ينبغي على مديري تقنية المعلومات التنفيذيين محاولة معرفة كيف يمكنهم خدمة مستخدميهم بصورة أفضل.
- كيف يمكننا وضع محفظة للاستثمارات الإستراتيجية؟ فبدلاً من مجرد تقديم طلبات الميزانية بانتظام فيما يخص مسائل مثل ترقية البرمجيات، هل يتم تقييم وتبرير مثل هذه الطلبات بعناية من قبل إدارة تقنية المعلومات؟
- كيف ينبغي أن نحدد جودة الخدمة؟ من خلال المسوحات والعمل التعاوني، هل كل الأطراف المعنية تدرك مدى الخدمات عالية الجودة التي تقدمها تقنية المعلومات؟
- كيف يمكننا تخصيص مواردنا بكفاءة من خلال محفظة مُعرّفة لدينا من الخدمات المقدمة؟
- كيف يمكننا حل الطلبات المتعارضة بالنسبة للخدمات المشتركة؟

وعلى الرغم من أن مفهوم الضوابط العامة لتقنية المعلومات موجود منذ الأيام الأولى للحاسبات المركزية، فإننا اليوم نستخدم غالباً مفهوم البنية التحتية لتقنية المعلومات للإشارة إلى مجموعة العمليات التي تشمل جميع العمليات التشغيلية المتعلقة بتقنية المعلومات في المؤسسة. ستكون هناك اختلافات كبيرة جداً بين البنى التحتية لتقنية المعلومات الخاصة

بالعديد من المؤسسات الكبيرة والصغيرة اعتماداً على الحجم النسبي لعملياتها التشغيلية وطبيعة أعمالها بشكل عام. ونظراً للعديد من هذه الاختلافات المحتملة في أنواع وأحجام نظم ومرافق تقنية المعلومات والتي قد تكون ضرورية في هذه الحالة، فإنه في الحقيقة لا يوجد هنا مجموعة واحدة من إجراءات رقابة صحيحة وأخرى خاطئة. ولكن ينبغي على المؤسسة أن تحدد وتطبق مجموعة من أفضل الممارسات التي من شأنها أن تكون بمثابة إرشادات لوضع الضوابط العامة لتقنية المعلومات الخاصة بها.

في جميع الأحوال فإن المفهوم الهام للرقابة الداخلية هنا، يتجاوز غالباً الكيفية التي يتم من خلالها إيصال تقارير تطبيقات تقنية المعلومات والمخرجات الأخرى لتقنية المعلومات ليصل إلى مستخدمي الأعمال لديها. حيث تقوم كل إدارة من إدارات تقنية المعلومات بدعم مجموعة واسعة من عمليات إدارة خدمات تقنية المعلومات التي تم تعريفها بواسطة آيتل والتي تضمنت مجالات مثل إدارة المشاكل (بمعنى أنه كيف تقوم إدارة تقنية المعلومات بحل المسائل والقضايا المتعلقة بمستخدمي الأعمال لديها) وإدارة التهيئة (بمعنى أنه كيف تقوم إدارة تقنية المعلومات بمتابعة إصدارات البرمجيات والمعدات المستخدمة لديها والاحتفاظ بها في أحد السجلات). تشمل إدارة خدمات تقنية المعلومات على عدد كبير من قضايا الرقابة الداخلية، وبدلاً من الحديث عن إيجابيات وأخطاء عملية محددة، فهناك بعض الممارسات المثلى المتعارف عليها والتي يجب على المؤسسة أن تقوم باستخدامها. حيث يعد التطبيق الفعال لأفضل الممارسات الموجودة في آيتل أحد العناصر المهمة في الممارسات الشاملة الجيدة لحوكمة تقنية المعلومات.

تعد الإدارة المالية لخدمات تقنية المعلومات أحد المجالات التي يتم تجاهلها غالباً من قبل الإدارة المالية وإدارة تقنية المعلومات. إن أفضل الممارسات لإدارة الخدمة التي يوصي بها آيتل هي التي تحدد إطار العمل هنا، ويجب على وحدة تقنية المعلومات وإدارتها أن تضع في الحسبان قضايا الإدارة المالية أثناء قيامهم بتقييم مخاطر الضوابط الداخلية لتقنية المعلومات لديهم وتنفيذهم للتنقيحات والتحسينات الفعالة للضوابط العامة لتقنية المعلومات. ونظراً لعدم وجود تعريف محدد بشكل مطلق لما يسمى «أفضل»، فإن البعض يشير إلى تلك الممارسات باسم الممارسات الجيدة فقط.

وعلى الرغم من وجود العديد من إستراتيجيات إدارة الخدمة التي تم تحديدها ووصفها، فإن الإدارة المالية لخدمات ونظم تقنية المعلومات تعد من أفضل الممارسات الهامة لحوكمة تقنية المعلومات التي يتم تجاهلها غالباً من قبل الإدارة المالية وإدارة تقنية المعلومات في المؤسسة. وتعد مسألة الإدارة المالية لخدمات تقنية المعلومات واحدة من المجالات التي يتم تجنبها من قبل الأخصائيين المحترفين في تقنية المعلومات بحجة أنهم ليسوا محاسبين ولا يفهمون الأمور التي تتعلق بالمحاسبة باستثناء القيام بوضع ميزانية بسيطة، في حين أن الموظفين الاعتياديين في الإدارة المالية ينظرون غالباً إلى خدمات تقنية المعلومات على أنها قضية تقنية بحتة أو لا تتعدى اهتمامها وضع ميزانية أساسية. في جميع الأحوال، فإن مجال الإدارة المالية لخدمات تقنية المعلومات يعد أحد المجالات المهمة في الرقابة الداخلية التي تدعو للقلق وأحد أفضل الممارسات الموجودة في آيتل.

كانت إدارة تقنية المعلومات في معظم المؤسسات تعمل في أيامها الأولى كخدمة دعم "مجانية" بالإضافة إلى نفقاتها التي كانت تُعالج من خلال الإدارة المركزية وكذلك التكاليف المخصصة لصالح المستفيدين دون إيلاء المزيد من الاهتمام للتكاليف المتعلقة بتقنية المعلومات. فإذا ما أرادت إحدى إدارات المستخدمين طلب تطبيق جديد، فإنها ستقوم بالضغط على الإدارة لتمويل أعمال التطوير أو شراء حزم البرمجيات اللازمة وإضافة أي شخص من الأشخاص الذين لا بد من إضافتهم لإدارتها. مع مرور الوقت، بدأت إدارات تقنية المعلومات بوضع عمليات خاصة بتحميل التكاليف المرتبطة بخدمات تقنية المعلومات التي تقدمها وأعمال الدعم التي تقوم بها على المستفيدين، فإنه كان في الغالب ينظر إلى هذه العمليات على أنها سلسلة من المعاملات التي تقوم بجمع "أموال غير حقيقية" حيث لا أحد يولي المزيد من الاهتمام لموضوع التكاليف الفعلية لخدمات تقنية المعلومات وتسعيرها.

أما اليوم، فيجب أن يؤخذ موضوع التكاليف وتسعير خدمات تقنية المعلومات في الحسبان وإيلاء المزيد من الاهتمام به. كما يجب أن تعمل إدارة تقنية المعلومات المدارة بشكل جيد كما لو كانت وحدة أعمال تجارية، وتعد الإدارة المالية في آيتل إحدى العمليات الرئيسية الهامة التي تساعد على إدارة الضوابط المالية الخاصة بهذه الوحدة التجارية. إن الهدف من عملية الإدارة المالية في إستراتيجية الخدمة هو تقديم النصح والإرشاد الكافي

لإدارة الأصول والموارد المستخدمة في تقديم خدمات تقنية المعلومات على نحو جيد وفعال من حيث التكلفة. حيث من الواجب أن تكون إدارة تقنية المعلومات قادرة على حساب كامل نفقاتها التي تنفقها على خدمات تقنية المعلومات، وأن تقوم بتحميل هذه التكاليف الخاصة بالخدمات التي يتم تقديمها على عملاء المؤسسة المستفيدين منها. وهناك ثلاثة عمليات فرعية مستقلة ومرتبطة بالإدارة المالية في آيتل هي:

١- **وضع ميزانية لتقنية المعلومات** هي عملية توقع وضبط النفقات المالية على موارد تقنية المعلومات. تتضمن عملية تخصيص الميزانية دورة من المفاوضات التي تتكرر عادة كل سنة، لتحديد الميزانيات العامة إلى جانب الرقابة اليومية المستمرة للميزانيات الحالية. إن تخصيص الميزانيات يضمن أن يكون هناك تخطيط وتمويل ملائم للخدمات المناسبة لتقنية المعلومات وأن تعمل تقنية المعلومات في حدود تلك الميزانية خلال هذه الفترة. وسيكون لإدارات الأعمال الأخرى مفاوضات دورية مع تقنية المعلومات لوضع خطط الإنفاق والبرامج الاستثمارية المتفق عليها؛ وهي ما ستحدد في نهاية المطاف الميزانية التي سيتم تخصيصها لتقنية المعلومات.

٢- **محاسبة تقنية المعلومات** هي مجموعة من العمليات التي تمكن إدارة تقنية المعلومات من إجراء عملية حسابية كاملة للطريقة التي يتم من خلالها إنفاق أموالها على العملاء والخدمات والأنشطة. ولا تقوم إدارات تقنية المعلومات اليوم دائماً بعمل جيد في هذا المجال. فهي لديها مجموعة واسعة من التكاليف الخارجية، التي تتضمن البرمجيات، والاتفاقيات الخاصة باستئجار المعدات وتكاليف الاتصالات، وغيرها من النفقات، إلا أنه في كثير من الأحيان لا يتم إدارة هذه التكاليف أو الإبلاغ عنها بطريقة جيدة. كما أن لديها ما يكفي من البيانات اللازمة لدفع الفواتير وتقييم بعض التكاليف لمجالات محددة، إلا أن إدارات تقنية المعلومات غالباً ما تفتقر إلى مستوى أكثر تفصيلاً للحسابات، مثل محاسبة التكاليف أو نموذج المحاسبة القائم على النشاط الموجود في مؤسسات الإنتاج الكبرى.

٣- **المطالبة المالية** هي عمليات التسعير وإصدار الفواتير لمطالبة العملاء بالدفع مقابل الحصول على خدمات تقنية المعلومات التي يتم تقديمها لهم. وهذا يتطلب نظاماً محاسبياً سليماً لتقنية المعلومات، ويحتاج إلى أن يتم تطبيقه بطريقة بسيطة ونزيهة

ومحكمة جيداً. في بعض الأحيان يتم تقسيم عملية المطالبة بالأموال الخاصة بإحدى إدارات تقنية المعلومات بسبب شدة تعقيد تقارير الفواتير المتعلقة بخدمات تقنية المعلومات أو بسبب التقنية المتبعة التي يصعب على العديد من العملاء فهمها. تحتاج تقنية المعلومات إلى إصدار تقارير واضحة ومفهومة تتعلق بخدمات تقنية المعلومات المستخدمة بحيث تمكن العملاء من التحقق من تفاصيلها، وفهم ما يكفي للاستفسار عن الخدمات، والتفاوض بشأن التعديلات إذا لزم الأمر.

تقوم الإدارة المالية لتقنية المعلومات بدعم عملية إستراتيجية الخدمة من خلال هذه الإجراءات المحددة للتكاليف، والتسعير، والمطالبة. وعلى الرغم من أن هذه العملية للإدارة المالية لا تعمل عموماً على أنها مركز لتحقيق الأرباح، فإنها تسمح لكل من إدارة تقنية المعلومات وعملائها بالتفكير بشكل أفضل بالعمليات التشغيلية لخدمات تقنية المعلومات من الناحية التجارية. وقد تسمح عملية الإدارة المالية لإدارة تقنية المعلومات والإدارة بشكل عام باتخاذ قرارات تتعلق بتحديد الوظائف، إن وُجدت، والتي يجب الإبقاء عليها بداخل الشركة، والوظائف التي يجب إسنادها (تعهدتها) لمقدمي خدمات من خارج المؤسسة.

تسمح عملية الإدارة المالية في آيتل بإجراء تحليل دقيق لتكلفة خدمات تقنية المعلومات التي يتم تقديمها والعائد المادي منها، كما تسمح لإدارة تقنية المعلومات بوضع وتحقيق أهداف مالية محددة. كما أنها توفر التقارير الخاصة بعمليات إدارة مستوى الخدمات في الوقت المناسب، الأمر الذي يمكن العملاء من فهم الطرق المتبعة للمطالبات المالية وتسعير الخدمات. فمن بين جميع عمليات آيتل الخاصة بدعم وتقديم الخدمات، تعد عملية الإدارة المالية واحدة من أفضل الممارسات في آيتل التي يكون الاهتمام بها غالباً أقل من المستوى المطلوب. فالممول التقنية الموجودة لدى الأشخاص العاملين في تقنية المعلومات يدفعهم إلى التفكير بالإدارة المالية على أنها قضية محاسبية. على الجانب الآخر من العملة، فإن المهنيين العاملين بالمالية والمحاسبة يميلون إلى التفكير في هذه القضايا على أنها تقنية بحتة وأنها لا تتعدى مثل هذه المعاملات الخاصة بمحاسبة استئجار المعدات أو رسوم استئجار المرافق. إن تكاليف وأسعار خدمات تقنية المعلومات تعد من القضايا الهامة في حوكمة تقنية المعلومات.

تصميم الخدمة في آيتل:

هناك ثلاثة مجالات لعملية إستراتيجية الخدمة في آيتل في دورة حياة خدمة تقنية المعلومات، تبدأ بتصميم الخدمة، وكما هو مبين في الشكل التوضيحي (٦-١). فإن عمليات تصميم الخدمة في آيتل تغطي مجالات أكثر انسجاماً مع عمليات التشغيل السلسلة وذات الكفاءة للبنية التحتية لتقنية المعلومات بشكل عام. ويحدد آيتل خمسة جوانب لتصميم الخدمة:

- ١- تصميم كل خدمة من خدمات تقنية المعلومات التي يتم تقديمها، يشتمل على المتطلبات الوظيفية، والموارد الضرورية والقدرات المتوقعة.
 - ٢- تصميم نظم وأدوات إدارة الخدمة، يتم غالباً تقديمه عن طريق محفظة رسمية لإدارة وضبط هذه الخدمات خلال دورة حياتها.
 - ٣- تصميم النظم المعمارية والإدارية لتقنية المعلومات يعد أمراً ضرورياً لتوفير الخدمات.
 - ٤- تصميم العمليات يعد أمراً ضرورياً لترتيب وتشغيل وتحسين مجمل العمليات الخاصة بالخدمات.
 - ٥- تصميم أساليب قياس ومقاييس معيارية لعمليات الخدمات والبنية المعمارية لمكوناتها.
- إن ما يقوم آيتل بتعريفه على أنه خدمات العملاء يدل حقيقة على أن كل إدارة من إدارات تقنية المعلومات تنشئ الكثير من الخدمات للعملاء، وأنه لا بد من إدارة وضبط هذه الخدمات المعروضة من خلال حوكمة تقنية المعلومات المناسبة واستخدام التقنيات الخاصة بأفضل الممارسات. ولدعم عملية تقديم خدمات ذات كفاءة عالية، قام آيتل بتحديد مجموعة محددة من العمليات النوعية. كان البعض منها كعملية إدارة استمرارية أعمال تقنية المعلومات، مفضلاً لدى إدارة تقنية المعلومات ومدققها على مر السنين. كما أن هناك عمليات أخرى مثل اتفاقيات مستوى الخدمة Service Level Agreements (SLAs)، والتي تحدد الأداء والتوقعات المتفق عليها بين إدارة تقنية المعلومات وعملائها والتي لا يتم فهمها وتطبيقها دائماً كما ينبغي. وسيتم مناقشة اتفاقيات مستوى الخدمة في الفصل السابع عشر من هذا الكتاب.

إدارة السعة الخاصة بتقديم الخدمة:

تضمن إدارة السعة في آيتل أن تتماشى سعة البنية التحتية لتقنية المعلومات مع احتياجات العمل للحفاظ على المستوى المطلوب من تقديم الخدمات ضمن تكلفة معقولة ومنطقية من خلال مستويات مناسبة للسعة. فمن خلال جمع البيانات المتعلقة بسعة الأعمال والسعة التقنية، ينبغي أن تسفر هذه العملية من عمليات آيتل عن خطة مناسبة للسعة يتم من خلالها تقديم متطلبات خاصة بسعة تقنية المعلومات يمكن تبرير تكلفتها بالنسبة للمؤسسة. وبالإضافة إلى الهدف الأساسي لفهم المتطلبات الخاصة بسعة تقنية المعلومات في المؤسسة وتقديم مقابل لها (متطلبات - مميزات مقابل متطلبات)، فإن إدارة السعة هي المسؤولة عن تقييم المزايا المحتملة للتقنيات الجديدة التي يمكن أن تكون لدى المؤسسة.

تتكون عملية إدارة السعة في آيتل من ثلاث عمليات فرعية هي: إدارة سعة الأعمال وإدارة سعة الخدمة وإدارة سعة الموارد. بالنسبة لإدارة سعة الأعمال فهي عملية طويلة الأجل لضمان أخذ المتطلبات المستقبلية للأعمال بعين الاعتبار ومن ثم التخطيط لها وتنفيذها حسب الحاجة. أما إدارة سعة الخدمة فهي المسؤولة عن التأكد من أن أداء جميع خدمات تقنية المعلومات الحالية يتفق مع المعايير المحددة في اتفاقيات مستوى الخدمة (SLAs). وأخيراً، إدارة سعة الموارد، فهي تركز بصورة أكبر على الناحية التقنية وهي المسؤولة عن إدارة المكونات الفردية الموجودة في البنية التحتية لتقنية المعلومات. تشتمل المدخلات المتعددة لتلك العمليات الفرعية الخاصة بإدارة السعة على ما يلي:

- اتفاقيات مستوى الخدمة والخروقات الخاصة بها (وهذا ما سيتم تناوله بمزيد من المناقشة والتفصيل في الفصل السابع عشر من هذا الكتاب).
- خطط وإستراتيجيات العمل.
- الجداول الزمنية التشغيلية، إلى جانب إجراء تغييرات على الجدول.
- قضايا تطوير التطبيقات.
- القيود المفروضة على التقنية وعمليات الاستحواذ.

• حوادث ومشاكل تقنية المعلومات.

• الميزانيات والخطط المالية.

ونظراً لهذه المدخلات المتعددة، فإن عملية إدارة السعة تكون غالباً تحت إدارة مدير واحد مُعين لإدارة السعة، والذي يجب أن يدير عمليات تقنية المعلومات، ويقوم على تطوير وصيانة خطة رسمية لإدارة السعة، وأن يضمن تحديث السجلات الخاصة بالسعة. وبالإضافة إلى ذلك، لا بد من إشراك مدير السعة في عمليات تقييم جميع التغيرات ليحدد مدى تأثير التغيرات الجديدة على السعة والأداء. ولا بد من إجراء عملية التحقق من السعة أثناء اقتراح التعديلات وبعد تنفيذها. كما يجب أن تولي إدارة السعة اهتماماً خاصاً بالتأثير التراكمي للتغيرات على مدى فترة من الزمن والتي يمكن أن تسبب انخفاضاً في أوقات الاستجابة وحدوث مشاكل في عمليات تخزين الملفات وفي زيادة الطلب على السعة المستخدمة في عمليات المعالجة. وتشتمل المسؤوليات الأخرى المتعلقة بعملية إدارة السعة على بعض مهام مدير نظم الشبكات ومدير تطوير التطبيقات. فهم المسؤولون عن ترجمة متطلبات العمل إلى السعة اللازمة لتكون قادرة على تلبية هذه الاحتياجات وتحسين أداء تقنية المعلومات.

إن التطبيق الفعال لعملية إدارة السعة من شأنه أن يقدم لإدارة تقنية المعلومات فوائد، كتقديم ملخص حقيقي عن السعة المتاحة حالياً، والقدرة على التخطيط المسبق لحجم السعة المطلوبة مستقبلاً. ينبغي أن تكون الإدارة الفعالة للسعة قادرة على تقدير أثر التطبيقات أو التعديلات الجديدة على السعة، كما يجب عليها أن تقوم بتقليل التكاليف التي تتماشى مع متطلبات عمليات التشغيل في المؤسسة. إن التخطيط السليم للسعة يمكن أن يقلل بشكل كبير من التكلفة الإجمالية الناجمة عن اقتناء نظام تقنية المعلومات. فعلى الرغم من أن التخطيط الرسمي للسعة قد يتطلب الكثير من الوقت والموارد البشرية المتمثلة في فرق عمل داخلية وخارجية، وبرمجيات وأجهزة وأدوات، إلا أن الخسائر التي يمكن تكبدها جراء غياب التخطيط للسعة قد تكون كبيرة جداً. إن عدم إتاحة البيئة الإنتاجية للمستخدمين الذين يعملون في إدارات الأعمال الحساسة، والمبالغ الطائلة التي تنفق على معدات الشبكات أو الخدمات، والتكاليف المترتبة على عمليات ترقية النظم الموجودة حالياً بالفعل في البيئة الإنتاجية، كل ذلك قد يكون أكثر من مبرر للتكلفة الخاصة

بعملية التخطيط للسعة. ولأن هذه العملية تعد من العمليات الهامة في آيتل، لذا ينبغي هنا أن تقوم إدارة تقنية المعلومات بأخذ عمليات إدارة السعة المعمول بها والمتعارف عليها في الاعتبار عند قيامها بمراجعة عمليات حوكمة تقنية المعلومات.

يتحدث الفصل التاسع من هذا الكتاب عن المزيد من القضايا المتعلقة بإدارة سعة تقنية المعلومات من منظور الحوسبة السحابية Cloud Computing والافتراضية Virtualization. فالحوسبة السحابية Cloud Computing تشير إلى تلك الموارد الهائلة لتقنية المعلومات المتعددة الخوادم التي يتم توفيرها من قبل عدد متزايد من كبار الباعة. فنحن الآن في عصر تتوفر فيه الموارد التخزينية بأثمان رخيصة أكثر من أي وقت مضى، لذا فإننا نتحدث هنا عن كمية غير محدودة تقريباً من الموارد التخزينية الخاصة بتقنية المعلومات. أما الافتراضية Virtualization فهي من الموضوعات الأخرى التي لها علاقة بإدارة السعة وحوكمة تقنية المعلومات التي تم الحديث عنها ومناقشتها في الفصل التاسع من هذا الكتاب؛ حيث يشير مصطلح الافتراضية إلى الأدوات البرمجية التي يمكن من خلالها مشاركة أو تقاسم موارد تقنية المعلومات بطريقة لا تجعلنا نشعر بالقلق إزاء القيود المفروضة على الموارد في أي جهاز. وقد أسهمت هذه التقنيات في تغيير العديد من الطرق والأساليب المستخدمة، ومع ذلك فإن مفهوم إدارة السعة في آيتل ما زال يعد واحداً من المفاهيم الهامة في مجال حوكمة تقنية المعلومات.

إدارة الإتاحة للخدمات المقدمة:

ازداد اعتماد المؤسسات هذه الأيام على خدمات تقنية المعلومات المقدمة إليها والمتاحة سبعة أيام في الأسبوع و٢٤ ساعة في اليوم. في كثير من الحالات نرى أنه عندما تكون تلك الخدمات الخاصة بتقنية المعلومات غير متاحة، فإن الأعمال أيضاً تتوقف. ولذلك فإن قيام إدارة تقنية المعلومات بإدارة ومراقبة مدى إتاحة الخدمات التي تقدمها تعد من الأمور الحيوية. ويمكن تحقيق ذلك من خلال تحديد احتياجات الأعمال المتعلقة بموضوع إتاحة خدمات تقنية المعلومات، ومن ثم مقارنتها مع الإمكانيات المتوفرة لدى إدارة تقنية المعلومات.

تعتمد أفضل الممارسات الخاصة بإدارة الإتاحة في آيتل على عدة مدخلات، تتضمن المتطلبات المتعلقة بإتاحة الأعمال؛ معلومات عن الموثوقية أو الاعتمادية، والصيانة، والتعافي، وإمكانية تقديم الخدمة؛ ومعلومات من العمليات الأخرى والحوادث والمشاكل ومستويات الخدمة التي يتم تحقيقها. تتمثل أهداف عملية إدارة إتاحة الخدمات في:

- وضع خطة مناسبة ومحدثة لإتاحة الخدمات وصيانتها بحيث تعكس الحاجات الحالية والمستقبلية للمؤسسة.

- توفير الخدمات والإرشادات التوجيهية لكافة المجالات الأخرى في المؤسسة فيما يخص القضايا المتعلقة بإتاحة تقنية المعلومات.

- التأكد من أن الإنجازات التي تتعلق بإتاحة الخدمات تلبى الأهداف الموضوعة وزيادة، وذلك من خلال إدارة أداء الإتاحة بالنسبة للخدمات والموارد.

- المساعدة في تشخيص وحل الحوادث والمشاكل المتعلقة بالإتاحة.

- تقييم تأثير كل التغيرات على خطة الإتاحة والأداء والسعة لجميع الخدمات والموارد.

- ضمان تطبيق الإجراءات الوقائية في أي مكان تكون فيه تكلفة تلك الإجراءات مبررة.

ويمكن وصف الأنشطة المتعلقة بإدارة إتاحة الخدمات على أنها عبارة عن إجراءات للتخطيط والتحسين والقياس. حيث يتضمن نشاط التخطيط القيام بتحديد متطلبات الإتاحة لمعرفة ما إذا كان هناك إمكانية للوفاء بها والكيفية التي يمكن من خلالها تطبيق الإتاحة المطلوبة. إن عملية إدارة مستوى الخدمة، والتي سيتم تناولها بمزيد من التفصيل لاحقاً في الفصل السابع عشر من هذا الكتاب تعد من العمليات التي تبقى على تواصل مستمر بالأعمال والقادرة على تزويد إدارة الإتاحة ببعض التوقعات المناسبة بخصوص الإتاحة المطلوبة. قد يكون هناك توقعات غير واقعية في الأعمال بخصوص إتاحة تقنية المعلومات دون فهم ما يعنيه هذا من حيث القيمة الحقيقية. فمثلاً، قد يرغب مستخدمو الأعمال في توفير إتاحة بنسبة ٩٩,٩٪، وهم حتى الآن لا يدركون أن تكلفة هذا الأمر ستزيد بمقدار خمسة أضعاف تكلفة الإتاحة التي تتوفر بنسبة ٩٨٪ فقط. وتقع إدارة مثل هذه التوقعات على عاتق إدارة مستوى الخدمة وعملية إدارة الإتاحة.

الشكل التوضيحي (٦-٤) يوضح العلاقة بين الإتاحة والتكاليف. حيث يتضح أن الحفاظ على مستوى أساسي منخفض من الإتاحة الخاصة بتشغيل نظم تقنية المعلومات لن يكلف الكثير، في حال كانت تلك الإتاحة هي كل ما ستحصل عليه المؤسسة. ويجب على إدارة تقنية المعلومات أن تضع هذه العلاقة في الحسبان عند قيامها بمراجعة الضوابط وتقديم التوصيات.

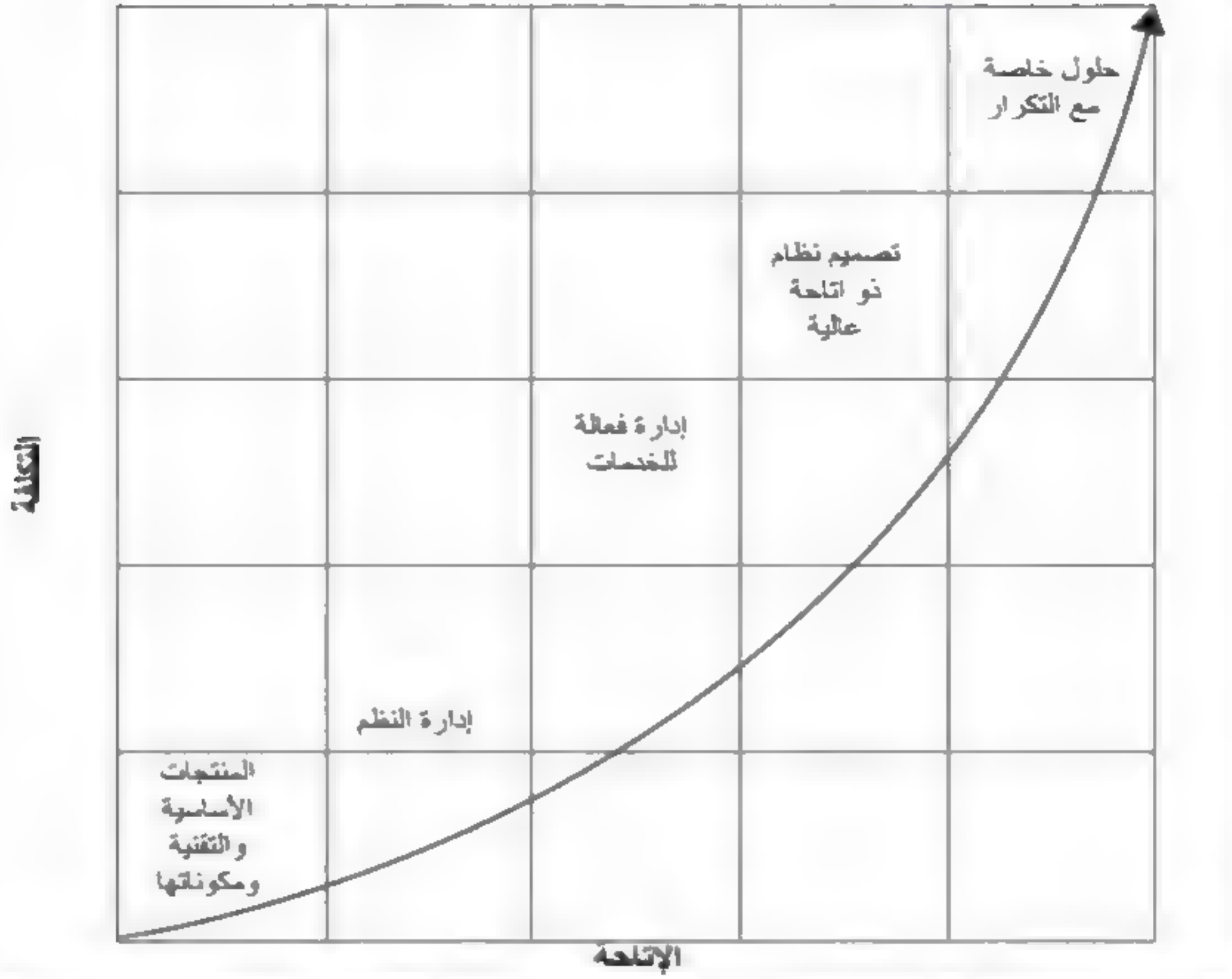
تستطيع إدارة تقنية المعلومات أن تقوم بتصميم إما عملية "إتاحة Availability" الخدمات أو عملية "استرجاع Recovery" الخدمات. فعندما لا تحتل الأعمال بقاء خدمة معينة معطلة لأي فترة من الزمن، فستكون إدارة تقنية المعلومات بحاجة إلى تعزيز المرونة في البنية التحتية التقنية الخاصة بها وضمان تنفيذ عمليات صيانة وقائية للمحافظة على استمرارية عمل الخدمات. وفي كثير من الحالات قد يكون بناء "إتاحة إضافية" "extra availability" في البنية التحتية مهمة باهظة الثمن ولكن يمكن تبريرها باحتياجات العمل. إن عملية التصميم لإتاحة الخدمات هي عبارة عن نهج استباقي لتفادي تعطل خدمات تقنية المعلومات.

أما إذا كانت الأعمال تستطيع تحمل توقف الخدمات لبعض الوقت، أو عندما لا يكون هناك أي مبررات لعمليات تعزيز إضافية في مرونة البنية التحتية التقنية، فإن وضع تصميم مناسب لاسترجاع الخدمات سيكون هو النهج المناسب. وفي هذه الحالة سيتم تصميم البنية التحتية بحيث أنه في حال توقف الخدمة ستبدأ عملية الاسترجاع في استعادة هذه الخدمة وتشغيلها "في أسرع وقت ممكن". إذ إن وضع تصميم للاسترجاع يعد نهجاً إدارياً للإتاحة يعتمد بشكل كبير على رد الفعل. فعند وقوع أي حادث يجب أن تكون العمليات الأخرى في آيتل مثل إدارة الحوادث في موضع التنفيذ للقيام بعملية استرجاع الخدمة وتشغيلها بأسرع ما يمكن في حال توقفها أو انقطاعها.

إن الفائدة الرئيسية من إدارة الإتاحة هو امتلاك عملية منظمة لتقديم الخدمات التي يتم توفيرها وفقاً لحاجات العملاء المتفق عليها مسبقاً. الأمر الذي يجب أن يؤدي إلى زيادة إتاحة خدمات تقنية المعلومات وزيادة مستوى الرضا لدى العملاء. وهذا يغطي مساحة قد تسمح للمدققين على أعمال تقنية المعلومات بطرح بعض الأسئلة الصعبة على أنها جزء من عمليات مراجعة الضوابط العامة لتقنية المعلومات التي يقومون بها.

شكل توضيحي (٦-٤)

العلاقة بين الإتاحة والتكاليف في الآيتل



إدارة أمن واستمرارية نظم المعلومات الخاصة بتقديم الخدمة:

تمثل إدارة الأمن والاستمرارية عنصرين مستقلين من العناصر الخاصة بأفضل ممارسات تقديم الخدمة الموجودة في آيتل. ونظراً لاعتماد الأعمال الآن على تقنية المعلومات أكثر من أي وقت مضى، فإن حجم التأثير الناجم عن عدم إتاحة أي خدمة من خدمات تقنية المعلومات قد يزداد بشكل كبير. وفي كل مرة يتم فيها انخفاض مدى إتاحة الخدمات أو أدائها، لا يستطيع عملاء تقنية المعلومات مواصلة تنفيذ أعمالهم بالشكل الطبيعي. وهذا الاتجاه نحو الاعتماد الكبير على دعم تقنية المعلومات وخدماتها سوف يستمر وسيؤثر بشكل مباشر ومنتزاع على العملاء والمديرين وصناع القرار. وتؤكد إدارة الاستمرارية في آيتل أنه يجب تقدير مدى تأثير الفقد الكلي أو الجزئي لخدمات تقنية المعلومات، كما

يجب عليها أيضاً أن تقوم بوضع خطط استمرارية لضمان أن الأعمال، والبنية التحتية لتقنية المعلومات الداعمة لها، سوف تكون قادرة دائماً على الاستمرار في العمل.

يدعو آيتل إلى تطوير إستراتيجية مناسبة تحتوي على شيء من التوازن المثالي بين الخيارات المتعلقة بالحد من المخاطر وخيارات استرجاع الخدمات. وهذه الإستراتيجيات تشبه إلى حد ما بعض الإستراتيجيات الخاصة باستمرارية الأعمال والتعافي من الكوارث المذكورة في الفصل العاشر من هذا الكتاب. وباستخدام الأساليب المذكورة هناك، فإنه يجب على المنظمة أن تقوم بتطبيق مجموعة فعالة من العمليات الخاصة باستمرارية الخدمة.

أما إدارة أمن تقنية المعلومات فهي مجموعة أخرى من أفضل الممارسات في آيتل. فآيتل يقر بضرورة توفر عمليات لأمن المعلومات ضمن إطار حوكمة الشركات، وذلك لوضع توجه إستراتيجي للأنشطة الأمنية وضمان تنفيذ هذه الأنشطة. ويأتي أمن المعلومات كثيراً بعد التركيز على حوكمة تقنية المعلومات، حيث يؤكد آيتل أن أمن المعلومات أكثر من مجرد قضية تخص تقنية المعلومات، فهو أيضاً قضية إدارية. إن أهداف أمن تقنية المعلومات هي حماية مصالح أولئك الذين يعتمدون على المعلومات التي تقدمها تقنية المعلومات وحماية النظم والاتصالات المستخدمة لإيصال تلك المعلومات. ويتم تحقيق أمن المعلومات في آيتل من خلال الأهداف التالية:

- **هدف الإتاحة:** أن تكون المعلومات متاحة ويمكن استخدامها عند الطلب، وأن النظم التي تتيحها يمكنها أن تقاوم وبشكل مناسب الهجمات وتتعافى من الأعطال أو تمنع حدوثها.
- **هدف السرية:** يتم مراقبة المعلومات أو الكشف عنها فقط لأولئك الذين لديهم الحق في الاطلاع عليها.
- **هدف النزاهة أو السلامة:** أن تكون المعلومات كاملة ودقيقة ومحمية ضد التعديل غير المصرح به.
- **هدف الموثوقية وعدم التنصل:** أن تكون إجراءات الأعمال وكذلك تبادل المعلومات بين المؤسسات أو مع الشركاء يمكن الوثوق بها.

وتستمر إدارة أمن المعلومات في آيتل في تحديد أفضل الممارسات للوصول إلى نظام كامل لإدارة أمن المعلومات. فأفضل الممارسات الهامة جداً، والعمليات الفعالة لإدارة أمن المعلومات تشكل عنصراً هاماً من عناصر الحوكمة الفعالة لتقنية المعلومات.

عمليات إدارة انتقال الخدمة في آيتل:

كما يعلم مديرو ومحترفو تقنية المعلومات، أن العمليات التشغيلية الخاصة بتقنية المعلومات تكون دائماً عرضة للتغيرات الدورية التي تتم على المعدات والبرمجيات. وقد تنطوي هذه العمليات على تخطيط الانتقال السليم لإدخال مكونات جديدة، واختبارها والتحقق من صحتها قبل أي إطلاق لها في البيئة الإنتاجية، وكذلك إدارة التهيئة لمراقبة المخزون، والعلاقات بين أجهزة وخدمات تقنية المعلومات. وقد قام آيتل بتجميع هذه الممارسات تحت ما يطلق عليه اسم إدارة الانتقال، وهو المجال الذي يمكن أن يسلط الضوء على بعض مخاطر الرقابة الداخلية المؤثرة بالنسبة للعمليات التشغيلية للبنية التحتية لتقنية المعلومات. فمن الممكن على سبيل المثال أن يتم تثبيت أحد تطبيقات تقنية المعلومات بضوابط داخلية غير مرنة. فضلاً عن أنه، من الممكن أن تتسبب التغيرات اللاحقة غير المصرح بها على التطبيق نفسه أو التهيئة غير السليمة للمعدات الملحقة به بظهور مخاوف رقابية جديدة.

إدارة التغيير الخاصة بانتقال الخدمة:

ينتج غالباً عن عملية إدارة المشاكل التي تم الحديث عنها كجزء من العمليات التشغيلية للخدمات، الحاجة لإجراء بعض التغييرات أو التعديلات في تقنية المعلومات، كالتغييرات التي تطرأ على البرنامج أو التعديلات الطارئة على العملية أو الإجراء لتحسين الخدمات والحد من التكاليف. إن الهدف من إدارة التغيير في آيتل هو استخدام أساليب وإجراءات معيارية للتعامل الفعال والفوري مع التغييرات كافة، وذلك للتقليل من درجة تأثير تلك التغييرات في جودة وأداء الخدمات والعمليات يوماً بعد يوم. وتشمل عمليات إدارة التغيير في آيتل:

- معدات وبرمجيات نظم تقنية المعلومات.
- معدات الاتصالات والبرمجيات.
- جميع برمجيات التطبيقات.
- جميع الوثائق والإجراءات المتعلقة بعمليات تشغيل ودعم وصيانة النظم الحية.

وتعد النقطة الأخيرة مصدر قلق واهتمام بشكل خاص، إذ يتم غالباً تغيير أجهزة وبرمجيات تقنية المعلومات مع عدم الاهتمام بشكل كاف بتغيير الوثائق والبرامج الداعمة المرتبطة بتلك الأجهزة والبرمجيات. فالتغييرات التي تحدث على أي عنصر من عناصر تقنية المعلومات (مثل برمجيات التطبيقات أو الوثائق أو الإجراءات) يجب أن تخضع لعملية رسمية خاصة بإدارة التغيير. ومع ذلك تكون عملية إدارة التغيير غالباً عشوائية حتى في أحسن أحوالها. ومن الأمثلة على ذلك، أن تتم التغييرات على التطبيقات دون التفكير في آثارها على مجمل البنية التحتية لتقنية المعلومات، أو بروز تغييرات أخرى ناجمة عن الإصلاحات التي تقوم بها إدارة الحوادث، أو طلبات الإدارة العليا المتعلقة بإجراء بعض التغييرات اللازمة لحل بعض المشاكل قصيرة الأجل أو الفورية. لذا ستعمل العمليات الرسمية لإدارة التغيير، والتي تقوم بمراجعة واعتماد التغييرات المقترحة، بشكل مستمر على تحسين عمليات تقنية المعلومات وعمليات الرقابة الداخلية في المؤسسة. وينبغي الربط بين عملية إدارة التغيير الموجودة في آيتل وإدارة التهيئة، التي تم الحديث عنها سابقاً، بشكل وثيق، وذلك لضمان إتاحة المعلومات الخاصة بالآثار المحتملة أو المترتبة على التغييرات المقترحة، والكشف عن أي تأثيرات محتملة وعرضها بشكل مناسب.

يجب أن يكون لعمليات إدارة التغيير رؤية عالية وقنوات اتصال مفتوحة من أجل تعزيز الانتقال السلس عند حدوث التغييرات. ولتحسين هذه العملية، قامت العديد من إدارات تقنية المعلومات بتشكيل مجلس استشاري رسمي للتغيير Change Advisory Board (CAB) مكون من مزيج من الأشخاص العاملين في إدارات تقنية المعلومات وإدارات المستخدمين الأخرى الموجودة بداخل المؤسسة، ليقوموا جميعاً بمراجعة التغييرات والموافقة عليها. فالمجلس الاستشاري للتغيير (CAB) هو كيان موجود للموافقة على التغييرات والمساعدة في تقييمها وتحديد أولوياتها. ويجب أن يُسند للمجلس مسؤولية التأكد من أن جميع التغييرات قد تم تقييمها بصورة كافية من منظور الأعمال والمنظور التقني. ولتحقيق هذا المزيج، يجب أن يكون المجلس الاستشاري للتغيير CAB مكوناً من فريق يعي بشكل جيد احتياجات أعمال العملاء إلى جانب الوظائف التقنية الخاصة بالدعم والتطوير. يرأس المجلس الاستشاري للتغيير (CAB) مدير مسئول عن عمليات التغيير، ويجب أن يضم المجلس كلاً من عملاء تقنية المعلومات، ومطوري التطبيقات، ومختلف الخبراء / الاستشاريين الفنيين

إذا اقتضت الحاجة ذلك، وممثلين عن المقاولين أو الأطراف الخارجية في حال كان هناك استعانة بمصادر خارجية. وعلى الرغم من أنه يجب على هذا المجلس أن يعقد اجتماعات دورية منتظمة لمراجعة وجدولة التغييرات المقترحة، فإنه لا ينبغي أن يكون بمثابة عائق أمام العمليات التشغيلية لتقنية المعلومات، بل لا بد من وجود هذا المجلس لتوفير جدولة منتظمة وإدخال جميع أنواع التغييرات على البنية التحتية لتقنية المعلومات.

تحتاج العمليات الشاملة الفعالة لإدارة الخدمات إلى القدرة على تغيير الأمور بطريقة منظمة، لتفادي الوقوع في أخطاء واتخاذ قرارات خاطئة. إن العملية الفعالة لإدارة التغيير أمر لا غنى عنه بالنسبة لبنية تحتية فعالة لتقنية المعلومات، وينبغي أن تشمل ما يلي:

- تحسين المواءمة والانسجام بين خدمات تقنية المعلومات ومتطلبات العمل.
- الشفافية المتزايدة ووضوح الرؤية والتواصل بشأن التغييرات لكل من فريق دعم الأعمال والخدمات.

- تحسين تقييمات المخاطر.

- تقليل التأثير السلبي للتغييرات على جودة الخدمات.

- تقييم أفضل لتكاليف التغييرات المقترحة قبل أن يتم تكبد تلك التكاليف.

- زيادة إنتاجية عملاء تقنية المعلومات من خلال تقليل أوقات الانقطاع وخدمات عالية الجودة.

- زيادة قدرة تقنية المعلومات لاستيعاب حجم كبير من التغييرات.

إن عملية إدارة التغيير في آيتل تعد عنصراً هاماً من عناصر البنية التحتية لتقنية المعلومات، وينبغي أن ترتبط وتتماشى بشكل وثيق مع العمليات الرئيسية لإدارة التهيئة والسعة والإطلاق في البنية التحتية لتقنية المعلومات. وهي أيضاً عنصر هام من عناصر الحوكمة الفعالة لتقنية المعلومات.

إدارة التهيئة الخاصة بانتقال الخدمة:

مهما كان حجمها النسبي، فإن الإدارات الخاصة بتشغيل تقنية المعلومات تعتبر معقدة، وذلك في ظل وجود العديد من الأنواع والإصدارات الخاصة بالمكونات المادية والبرمجية، هذا بالإضافة إلى الروابط المستخدمة للاتصال بمكونات الحوسبة السحابية، التي يجب أن تعمل جميعها معاً بطريقة منظمة ومحكمة الإدارة. ومن المؤكد أن هذا صحيح بالنسبة للشركة التي تعمل من خلال نظم أجهزة الحاسب المركزية Mainframes التقليدية، أو "مزارع" الخوادم "Farms of Servers"، وعدد كبير من أجهزة التخزين ومعدات الاتصالات، والأمر نفسه يسري على وحدة التشغيل الصغيرة لنظم تقنية المعلومات. تعد الوظيفة الرسمية لإدارة التهيئة عملية هامة لتقديم الخدمات التي تدعم التعريف والتسجيل والإبلاغ عن مكونات تقنية المعلومات وإصداراتها ومكوناتها التأسيسية وعلاقاتها. فالعناصر التي يجب أن تخضع لرقابة إدارة التهيئة تشمل الأجهزة والبرامج والوثائق المرتبطة بها. هناك اختلاف بين مفهوم إدارة التهيئة والمفهوم الخاص بعملية المحاسبة الإهلاكية الخاصة بإدارة الأصول، على الرغم من وجود علاقة بينهما. فنظم إدارة الأصول تحتفظ بتفاصيل عن معدات تقنية المعلومات التي تزيد قيمتها عن حد معين، ووحدة العمل والمواقع التي توجد بها. في حين تحتفظ إدارة التهيئة أيضاً بمعلومات عن العلاقات الموجودة بين الأصول، والتي لا تحتفظ بها إدارة الأصول عادة. فبعض المؤسسات تبدأ بإدارة الأصول ومن ثم تنتقل إلى إدارة التهيئة.

إن النشاط الأساسي والمهم لحوكمة تقنية المعلومات فيما يخص إدارة التهيئة هو تحديد المكونات المستقلة المختلفة للعمليات التشغيلية لتقنية المعلومات، والتي يطلق عليها اسم عناصر التهيئة (CIs)، ومن ثم تحديد البيانات الرئيسية الداعمة لهذه العناصر (CIs)، متضمناً ذلك "أصحابها"، وتحديد البيانات، وأرقام الإصدارات وكذلك العلاقات المتبادلة للنظم. ولا بد من الحصول على هذه البيانات وتنظيمها وحفظها في قاعدة بيانات تُعرف باسم قاعدة بيانات إدارة التهيئة Configuration Management Database (CMDB). ويجب على الفريق المسؤول عن إدارة التهيئة أن يقوم باختيار وتعريف هياكل التهيئة الخاصة بعناصر تهيئة البنية التحتية بأكملها، متضمناً ذلك تحديد العلاقات الموجودة بين

جميع عناصر التهيئة (CIs) والمكونات المتصلة في التهيئة الخاصة بمجمل البنية التحتية لتقنية المعلومات. وبالانتقال إلى ما هو أبعد من مجرد عملية إدخال البيانات في قاعدة بيانات إدارة التهيئة، فإنه يجب أن تضمن العملية أن عناصر التهيئة المصرح بها فقط هي التي يتم قبولها، كما يجب أن تضمن أيضاً عدم إضافة أي عنصر من عناصر التهيئة أو تعديله أو استبداله أو إزالته دون أن يكون هناك طلب سليم واضح لإجراء التغيير وبمواصفات محدثة.

يجب علينا التفكير في أهمية عملية إدارة التهيئة من حيث وجود التطبيقات الخاصة بتقنية المعلومات في إدارة الأعمال التقليدية. فربما يكون لدى كل عضو من أعضاء الطاقم الوظيفي هاتف ذكي أو جهاز حاسب محمول، وفي حال عدم وجود إصدارات متناسقة من البرامج الموضوعة على كل جهاز من هذه الأجهزة، فمن الممكن أن تكون هناك صعوبات في عملية اتصال تلك النظم بعضها مع بعض. هذا يفسر أهمية إدارة التهيئة. فمن المهم حقاً أن يكون لديك فهم لمختلف الإصدارات أو حتى الأنواع المتعددة للبرمجيات والمعدات في إدارات التشغيل الكبيرة لتقنية المعلومات.

تتضمن عملية إدارة التهيئة عناصر تحكم مهمة بالنسبة لمجمل عملية حوكمة تقنية المعلومات الفعالة. لذا يجب أن يحتفظ فريق تقنية المعلومات والمسؤول عن عملية إدارة التهيئة بسجلات عن حالة كل عنصر من عناصر التهيئة (CI) وتتبع حالته عندما تتغير من حالة لأخرى، فعلى سبيل المثال، قد تتغير حالة العنصر من مرحلة التطوير إلى مرحلة الاختبار، ومن ثم إلى مرحلة الإنتاجية، ومن ثم إلى مرحلة الإيقاف أو سحبه في نهاية الأمر. تعد قاعدة بيانات إدارة التهيئة مستودعاً لعناصر التهيئة، وليس من الضروري أن تكون قاعدة البيانات عبارة عن تطبيق معقد ومتخصص. فمثلاً، يمكن لأي مؤسسة أن تقوم بإنشاء قاعدة بيانات بسيطة لإدارة التهيئة CMDB فقط باستخدام جداول البيانات أو باستخدام نظم قواعد البيانات المحلية. وفي ظل وجود البنية التحتية الكبيرة والمعقدة لتقنية المعلومات اليوم، فإن إدارة التهيئة تتطلب غالباً استخدام المكتبات الطبيعية والإلكترونية جنباً إلى جنب مع قاعدة بيانات إدارة التهيئة للاحتفاظ بنسخ محددة لجميع البرامج والوثائق الداعمة. وينبغي أن تستند قاعدة بيانات إدارة

التهيئة إلى تقنية قاعدة البيانات التي توفر وسائل استعلام مرنة وقوية وتحدد العلاقات بين جميع مكونات النظام.

ترتبط عملية إدارة التهيئة مباشرة بعمليات إدارة تطوير واختبار وتغيير وإطلاق النظم للجمع بين المنتجات الجديدة والمحدثة. وبالإضافة إلى ذلك، فإن قاعدة بيانات إدارة التهيئة CMDB يمكن استخدامها من قبل عملية إدارة مستوى الخدمة للاحتفاظ بتفاصيل الخدمات وربط هذه الخدمات مع مكونات تقنية المعلومات التابعة لها. كما يمكن أيضاً أن تُستخدم قاعدة بيانات إدارة التهيئة لتخزين تفاصيل المخزون الخاصة بعناصر التهيئة CIs، مثل المورد، والتكلفة، وتاريخ الشراء، وتاريخ تجديد الترخيص. كما أن هناك ميزة إضافية تتمثل في استخدام قاعدة بيانات إدارة التهيئة لتغطية الجوانب القانونية المرتبطة بالحفاظ على التراخيص والعقود.

عمليات تشغيل الخدمة في آيتل:

لقد بدأت أفضل ممارسات آيتل الموصوفة في هذا الفصل بأهمية وضع إستراتيجيات للخدمة، والتي تتضمن السياسات الرئيسية لتقنية المعلومات والمجالات ذات المستوى العالي كالإدارة المالية لتقنية المعلومات. أما بالنسبة للعملية الاعتيادية الخاصة بإطلاق موارد تقنية المعلومات، فإن المجموعة التالية من أفضل الممارسات تغطي تصميم الخدمة، وهي العمليات التي تتناول سعة وإتاحة تقنية المعلومات، وكذلك إدارة مستوى الخدمة لتتفق مع مستخدمي خدمات تقنية المعلومات فيما يتعلق بالخدمات التي سيتم تقديمها. ويطلق على هذه العمليات الثلاث الأخيرة في آيتل اسم عمليات تشغيل الخدمة، وهي العملية التي تتيح لعملاء الأعمال رؤية جودة خدمات تقنية المعلومات التي يتم تقديمها.

تتضمن العمليات التشغيلية للخدمات القيمة اليومية للخدمات التي ينبغي تقديمها بواسطة نظم وعمليات تقنية المعلومات. إن الغرض من عملية تشغيل الخدمة في آيتل هو المساعدة في تنسيق وتقديم خدمات تقنية المعلومات للعملاء. كان هذا هو مفهوم القيمة الذي كان غالباً مفقوداً في الأيام الأولى لعمليات تشغيل تقنية المعلومات، إلا أن أفضل الممارسات في آيتل قد قامت بتقريب هذه المفاهيم المتعلقة باحتياجات العمل والإدارة.

تحدد عمليات تشغيل الخدمة في آيتل عمليات منفصلة لتشغيل الخدمة، وذلك فيما يخص إدارة الأحداث events والحوادث incidents، حيث يتم تعريف الأحداث على أنها أي واقعة يمكن اكتشافها ويكون لها تأثير في إدارة البنية التحتية لتقنية المعلومات أو تقديم الخدمات المتعلقة بتقنية المعلومات. وعلى الرغم من أن آيتل يحدد العديد من أوجه الشبه بين ما يسمى الأحداث والحوادث في آيتل إلا أن نقاشنا هنا سوف يركز على إدارة الحوادث (الأعطال)، ذلك أن التنفيذ الفعال لهذه العمليات سوف يحسن من مجمل عمليات التشغيل الخاصة بحوكمة تقنية المعلومات.

إدارة الأحداث والحوادث الخاصة بتشغيل الخدمة:

تتضمن عمليات إدارة الحوادث جميع الأنشطة اللازمة لاستعادة خدمات تقنية المعلومات بعد انقطاعها. يعرف آيتل الانقطاع أو العطل على أنه أي نوع من أنواع المشاكل التي قد تحرم مستخدم تقنية المعلومات من الحصول على الخدمات المناسبة المتوقعة، سواء كانت توقفاً لكامل النظام أم عدم قدرة المستخدم على الوصول إلى تطبيق ما لأي سبب من الأسباب الكثيرة جداً، أو عدم نجاح عملية الدخول بسبب خطأ مطبعي في كتابة كلمة المرور ناجم عن مشكلة "زلات الأصابع" ("Fat Fingers" أو أي مشكلة أخرى. ويطلق على المشكلة المبلغ عنها اسم الحادثة، وهي نوع من أنواع الانحراف عن عمليات التشغيل القياسية. وعلى الرغم من أن العديد من إدارات تشغيل تقنية المعلومات تمتلك إدارة تسمى مكتب المساعدة أو مجموعة دعم العملاء، فإن هذه الإدارة العامة يشار إليها هنا باسم مكتب الخدمة. فمكتب الخدمة يكون عادةً هو صاحب عملية إدارة الحوادث، على الرغم من أن كل مجموعات دعم الخدمات عبر تقنية المعلومات قد يكون لها دور في إدارة الحوادث.

إن الهدف من العمليات الفعالة لإدارة الحوادث هو استعادة العمليات التشغيلية الاعتيادية في أسرع وقت ممكن وبطريقة فعالة من حيث التكلفة وبأقل تأثير ممكن، سواء كان التأثير في الأعمال بكاملها أم في المستخدمين. ولا ينبغي أن يكون ما تعنيه "السرعة" هنا موضعاً للتأويل أو التفسير، حيث يدعو آيتل إلى تحديد المعايير الخاصة بالإطار الزمني لاستعادة الخدمات في اتفاقيات مستوى الخدمة التي تحدثنا عنها في الفصل السابع عشر

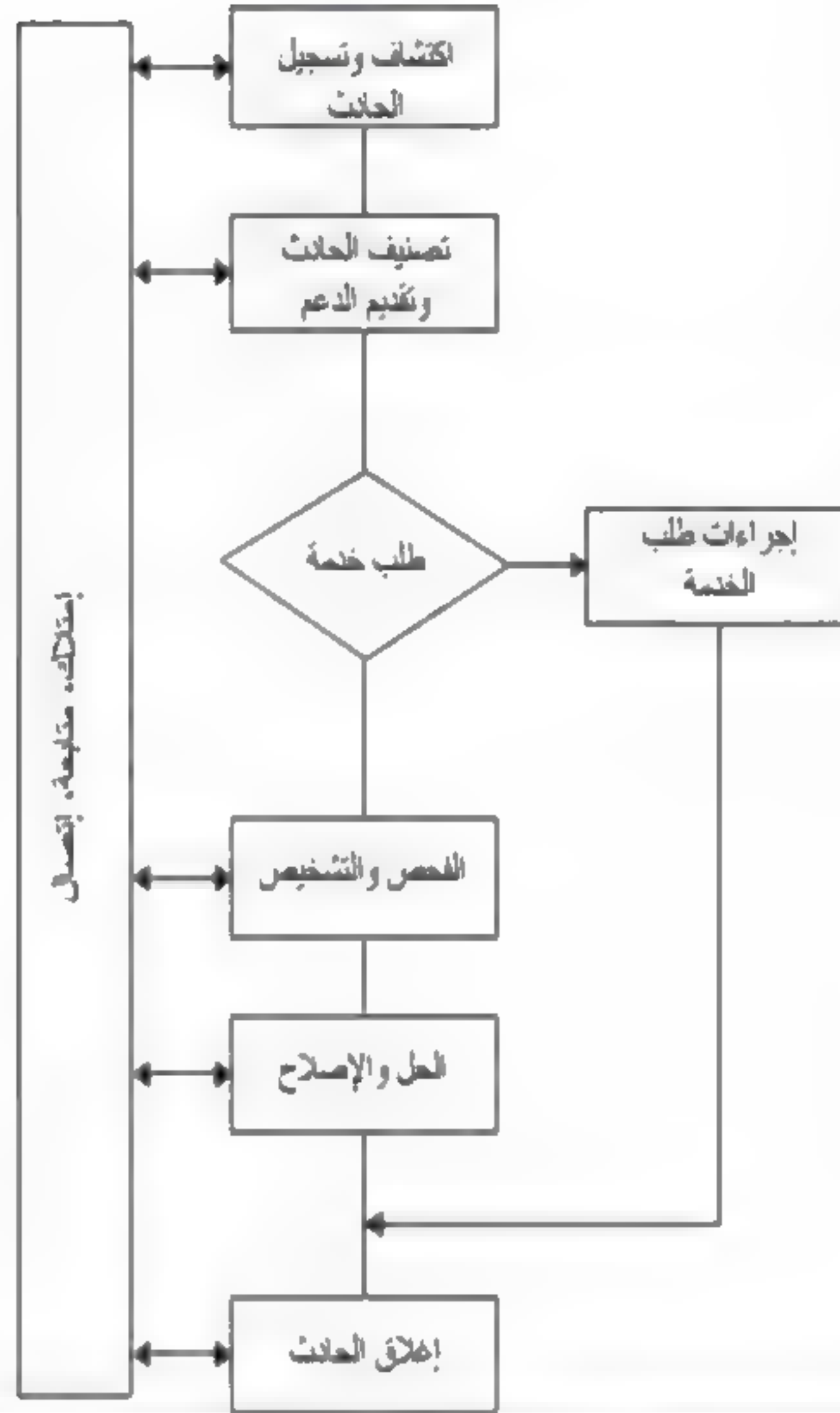
(*) هي مشكلة تقع نتيجة مدخلات خاطئة من خلال لوحة مفاتيح الحاسب الآلي (المترجم).

من هذا الكتاب. إن الاتفاقيات الفعالة لمستوى الخدمات SLAs هي إحدى المكونات الهامة في البنية التحتية لتقنية المعلومات، فوجودها مهم بالنسبة للممارسات الخاصة بحوكمة تقنية المعلومات. فالعنصر الأول في عملية إدارة الحوادث في آيتل هو اكتشاف الحادثة وتوثيقها من قبل مكتب الخدمة، كونه النقطة الوحيدة للاتصال. ويمكن أن تشمل هذه الحوادث مسائل مثل أن يقوم المستخدم بالاتصال بسبب وجود مشاكل معينة في التطبيق أو أن تقوم العمليات التشغيلية لتقنية المعلومات بإعلام مكتب الخدمة بإحدى المشاكل المتعلقة بمعالجة التطبيق.

بمجرد استلام الحادثة، يجب أن يقوم مكتب الخدمة بتصنيفها من حيث أولويتها priority، وأثرها impact، وإلحاحيتها urgency. إذ إن تحديد أولويات للحوادث المبلغ عنها يعد واحداً من أكثر القضايا الهامة في إدارة حوادث تقنية المعلومات. فكل شخص يبلغ عن حادثة يعتقد بأنها الأهم على الإطلاق، لذلك فوحدة إدارة الحوادث لديها مهمة صعبة تتمثل في تحديد الأولوية النسبية للحدث المبلغ عنه وأهميته، وتأثيره في العمل. الشكل التوضيحي (5-6) يلخص دورة الحياة لأحد حوادث تقنية المعلومات ابتداءً من الاتصال الأولي وصولاً إلى الحل والإغلاق. والنقطة الأساسية هنا هي أن نفهم أفضل الممارسات الموصى بها والخاصة بمكاتب الخدمة وأن نبحث عن الاتفاقيات الرسمية لمستوى الخدمات، على أنها جزء من عملية إدارة مستوى الخدمة، وذلك لتحديد أولويات الحوادث التي تحتاج إلى حل، والجهود المبذولة في حلها، والتعافي من الحوادث. يجب أن تعتمد اتفاقيات مستوى الخدمة على مدى تأثير أو مدى حساسية الحادث على وحدة الأعمال التي قامت بالتبليغ عنه أو على المؤسسة بأكملها. فيجب على سبيل المثال أن تقوم إدارة الحوادث بتقدير عدد المستخدمين المتضررين جراء العطل المبلغ عنه والخاص بإحدى المعدات أو الأجهزة المادية. وبالطريقة نفسها، فإن الإبلاغ عن مشكلة تتعلق بعملية الإقفال المحاسبي في نهاية الشهر يجب أن تحدد له درجة أهمية أعلى من الإبلاغ عن مشكلة تتعلق بتطبيق يقوم بإصدار أوامر الشراء.

شكل توضيحي (٥-٦)

دورة حياة إدارة الحوادث في الآيتل



أضف إلى ذلك، أنه ينبغي لفت الانتباه إلى إلحاحية الحادث المبلغ عنه. حيث تشير الإلحاحية إلى السرعة اللازمة لحل حادثة لها تأثير معين. ولا يتعين دائماً حل الحوادث الكبيرة الأثر بشكل فوري أو افتراضي. في الغالب يكون الإبلاغ عن الحوادث التي تفيد بأن مجموعة كبيرة من المستخدمين لا يستطيعون العمل إطلاقاً جراء بعض الانقطاعات في الخدمات تكون له درجة إلحاحية أكبر من الإبلاغ الذي يقوم به أحد كبار المديرين لطلب

تغيير وظيفة تشغيلية معينة. لذا يجب على فريق إدارة الحوادث التحقيق في الحوادث المبلغ عنها في أقرب وقت ممكن لتحديد مداها وتأثيرها. وربما يدل إخفاق أحد المكونات الذي يتم التبليغ عنه على أن هذا الجهاز خارج الخدمة أو أنه متوقف عن العمل. ويكون هذا النوع غالباً من الحوادث غير معقد كثيراً ونسبياً يمكن إصلاحه بسهولة. في حين قد يكون فشل الاتصالات، الذي ربما يؤثر في العديد من وحدات الأعمال الدولية ومن ثم ربما يؤخر الإقفال المالي الشهري، أكبر بكثير من حيث الحجم والنطاق.

وبمجرد تسجيل الحادث، يجب أن تبدأ عملية التحقيق والتشخيص. فإن لم يتمكن مكتب الخدمة من حل الحادث، فإنه يجب أن يُحيله إلى مستويات أخرى من الدعم الفني الخاص بتقنية المعلومات ليقوموا بحلها. وعلى أي حال، ينبغي على جميع الأطراف التي تعمل على الحادث الاحتفاظ بالسجلات المتعلقة بالإجراءات التي يقومون بها، وذلك من خلال التعديل على ملف مشترك خاص بتسجيل الحوادث. إذ يمكن حل بعض الحوادث من خلال عملية الإصلاح السريع التي يقوم بها مكتب الخدمة، والبعض الآخر يكون من خلال قرارات أكثر رسمية، أما في حالة المشاكل الأكثر أهمية، فيكون الحل من خلال اتباع الحلول البديلة لإعادة الأمور إلى نصابها من خلال عملية جزئية والمطالبة بتقديم طلب رسمي Request For Change (RFC) لتغيير النظم أو البائع أو أي شيء نحتاجه إلى إصلاح مثل هذه المشاكل ذات الأهمية الكبيرة. وعند وقوع أي حادث، لا بد من تنظيم الجهود الإصلاحية المبذولة لحل المشكلة وتنسيقها مع وحدة إدارة الحوادث المالكة للمسألة إلى أن يتم إيجاد الحل. ولا بد من الاحتفاظ بالوثائق السليمة للقيام بتتبع الحادث إلى أن يتم حله. وقد يتم إغلاق الحادث رسمياً بمجرد أن يتم إصلاح الأمور. أو إذا لم يحل بسهولة فإن الحادث يجب أن يُمرر إلى الوحدة المختصة بعملية إدارة المشاكل كما سنوضح لاحقاً.

ترتبط جميع عمليات آيتل إلى حد ما بعضها مع بعض، ولكن في العديد من الحالات تمثل إدارة الحوادث خط الدعم الأول بين مستخدمي أو عملاء خدمات تقنية المعلومات وإدارة تقنية المعلومات نفسها. لذا يجب أن تكون إدارة الحوادث أكثر تنظيماً من "مكاتب المساعدة" التي كانت موجودة في السابق عندما كان المستخدمون الذين يقومون بالتبليغ عن المشاكل لا يحصلون في الغالب على المساعدة الكافية والتي ربما لا تتجاوز القيام بإعادة تعيين كلمة

المرو. إن إدارة الحوادث هي نقطة الاتصال الأولى بين العملاء - المستخدمين - وإدارة تقنية المعلومات بشكل عام. تنشأ الحوادث، نتيجة الأعطال أو الأخطاء في البنية التحتية لتقنية المعلومات، والتي تؤدي إلى انحرافات حقيقية أو محتملة في العمليات التشغيلية المخطط لها للخدمات. في بعض الأحيان ربما يكون سبب وقوع هذه الحوادث واضحاً ويمكن معالجته أو إصلاحه دون الحاجة إلى مزيد من التحقيقات. وفي حالات أخرى من الممكن أن يكون هناك حاجة لإجراء إصلاحات في المعدات أو البرمجيات. الأمر الذي يستغرق بعض الوقت لتنفيذه. قد تكون الحلول قصيرة المدى حلولاً بديلة للحدث، وهي تعد حلاً سريعاً للعودة إلى عملية التشغيل. أو قد تكون طلب تغيير (RFC) Request For Change رسمياً موجهاً لعملية إدارة التغيير لإزالة الخطأ. أحد الأمثلة على الحلول البديلة أو الحلول القصيرة المدى، هو مطالبة العميل بأن يقوم بإعادة تشغيل جهاز الحاسب الشخصي أو إعادة ضبط الإعدادات الخاصة بخطوط الاتصالات دون التطرق مباشرة إلى السبب الحقيقي لحدوث المشكلة.

عندما يكون السبب الحقيقي للحدث غير معروف، فإنه يكون من المناسب رفع سجل مشكلة لخطأ غير معروف في البنية التحتية. ويتم رفع سجل المشكلة فقط في حال كانت عمليات التحقيق مضمونة ومكفولة، ويكون من الواجب تقييم تأثيرها الفعلي والمحتمل. فنجاح معالجة سجل المشكلة سيؤدي إلى تحديد الخطأ الأساسي. ويمكن تحويل حالة السجل بعد ذلك إلى خطأ معروف بمجرد إيجاد حل بديل و / أو RFC.

إدارة المشاكل الخاصة بتشغيل الخدمة:

عندما تواجه عملية إدارة الحوادث انحراف نتيجة سبب أو علة غير معروفة، فإنه يجب أن تُمرر تلك الحادثة إلى عملية إدارة المشاكل في آيتل لحلها. والهدف من ذلك هو تقليل التأثير الكلي للمشاكل من خلال عملية رسمية للكشف والإصلاح، والقيام باتخاذ الإجراءات اللازمة لمنع تكرارها. إن عملية إدارة المشاكل هي الخطوة التالية في مدى أهمية بعض الحوادث المبلغ عنها، وينبغي النظر إلى هذه العملية من حيث ثلاث عمليات فرعية: إدارة مراقبة المشاكل وإدارة مراقبة الأخطاء والإدارة الرائدة للمشاكل. يعرف آيتل "المشكلة Problem" على أنها السبب الرئيسي غير المعروف ينتج عنه واحد أو أكثر من الحوادث، ويُعرف "الخطأ المعروف Known Error" على أنه مشكلة قد تم تشخيصها بنجاح وتعريف

الحل البديل لها. ليس ضرورياً أن تكون الفكرة هنا هي إيجاد وحدة إدارية ثانية في إدارة تقنية المعلومات لكي تستقبل الحوادث المبلغ عنها لدى مكتب المساعدة، ولكن الفكرة هي أن يُحدد متى وكيف يجب أن يتم تهمير بعض حوادث مكتب المساعدة المبلغ عنها إلى شخص أو سلطة أخرى لتشخيص المسألة المبلغ عنها بشكل أفضل والتعامل معها على أنها مشكلة. إن العملية الفعالة لإدارة المشكلة يمكنها أن تفعل الكثير لتحسين مجمل الخدمة المقدمة لعملاء تقنية المعلومات.

بالإضافة إلى حل أي حادث فردي يتم إرساله إلى عملية إدارة المشاكل، فإنه ينبغي على تقنية المعلومات أن تسعى لإيجاد عمليات لتحسين التحكم في المشاكل والأخطاء، متضمناً ذلك الحفاظ على البيانات للمساعدة في تحديد الاتجاهات واقتراح إجراءات محسنة للوقاية الاستباقية من المشاكل. لذا لا بد من الاحتفاظ بالمعلومات المتعلقة بالحلول و/أو الحلول البديلة الخاصة بالمشاكل التي تم حلها، بالإضافة إلى سجلات المشاكل المغلقة. في كثير من الحالات، قد تواجه إدارة المشاكل موقفاً يتطلب ضرورة الذهاب إلى خطوة أبعد وتقديم طلب تغيير RFC رسمي، إما من خلال إدارة تطوير تقنية المعلومات وإما من خلال بائع الأجهزة أو البرامج.

وتركز عملية إدارة المشاكل على إيجاد أنماط بين الحوادث والمشاكل والأخطاء المعروفة. إذ إن المراجعة التفصيلية لهذه الأنماط تسمح للمحلل بحل المشكلة عن طريق النظر في العديد من الاحتمالات وتقليصها إلى أن يصل إلى الحل، وهذا ما يسمى بتحليل "السبب الجذري" Root Cause. فهناك العديد من التقنيات الجيدة المستخدمة في حل وتصحيح المشاكل التي تكون غالباً نتيجة مجموعة من العوامل التقنية وغير التقنية. وتعد إدارة المشاكل مجالاً جيداً لتشخيص عمليات تقديم خدمات تقنية المعلومات من أجل تحقيق مستوى فهم أفضل للصحة العامة لعمليات تقنية المعلومات. ويمكن جمع المزيد من المعلومات من خلال فهم عدد طلبات التغيير RFCs التي تم رفعها، ومدى تأثير تلك الطلبات في إتاحة وموثوقية الخدمات كافة المقدمة في تقنية المعلومات، ومقدار الوقت المستغرق في عمل التحقيقات والتشخيص لأنواع مختلفة من المشاكل عن طريق الوحدة التنظيمية أو البائع، وعدد وتأثير الحوادث التي تقع قبل أن يتم حل المشكلة الجذرية أو تأكيد الخطأ المعروف، والخطط من أجل حل المشاكل المفتوحة فيما يتعلق بالأفراد

والاحتياجات الأخرى من الموارد، وكذلك التكاليف ذات الصلة والمبالغ المرصودة في الميزانية. تعد عمليات إدارة المشاكل الخاصة بتشغيل خدمات تقنية المعلومات في آيتل من الأمور الهامة من أجل فهم وتقييم الصحة العامة لعمليات تشغيل البنية التحتية لتقنية المعلومات. فالعملية الفعالة لإدارة الحوادث تكون ضرورية لاستقبال مكالمات العملاء واتخاذ الإجراءات التصحيحية الفورية، في حين أن عملية الإدارة الفعالة للمشاكل قد تذهب خطوة أبعد من ذلك حيث تعمل على تحليل وحل المشكلة من خلال البدء في تقديم طلبات التغيير RFCs عند الضرورة، وفيما عدا ذلك فإنها تعمل على تحسين رضا العملاء.

حوكمة تقنية المعلومات وأفضل ممارسات تقديم الخدمة في آيتل:

أوجزت الفقرات السابقة بعض عمليات دورة حياة إدارة الخدمة الأكثر أهمية في آيتل. حيث تقوم إدارة الخدمات في آيتل بوضع الخطوط العريضة لعمليات إطلاق وإدارة وضبط جميع مستويات خدمات تقنية المعلومات مع التأكيد على تحقيق رضا العميل. إن إرشادات آيتل تذهب إلى ما هو أبعد من الرقابة الداخلية، فهي تشمل إدارة تكاليف تقنية المعلومات، ووضع القياسات والمقاييس، وغيرها من قياسات تحسين الجودة.

يدعو آيتل أي إدارة من إدارات تقنية المعلومات إلى أن تقوم ببناء برنامج للتحسين المستمر للخدمات من أجل مراجعة وتحليل وتقديم توصيات بشأن فرص التحسين في كل مرحلة من مراحل دورة حياة تقديم الخدمات في آيتل والتي تمت مناقشتها في هذه الأقسام. إن عمليات دورة حياة إدارة الخدمة في آيتل قد تم اعتمادها بشكل متزايد من خلال إدارات تقنية المعلومات في جميع أنحاء العالم. إذ إن التركيز على الخدمة يرفع أهمية موارد تقنية المعلومات والبنية التحتية الداعمة لها بالنسبة للمؤسسة بكاملها وعملائها وأصحاب المصلحة فيها.

إن دورة حياة إدارة الخدمة في آيتل عبارة عن سلسلة من العمليات المترابطة لأفضل الممارسات التي تدعم إدارة البنية التحتية لتقنية المعلومات وإدارة المؤسسة. إن تطبيقات تقنية المعلومات تقع في وسط هذه المعضلة وتمثل منطقة مركزية رئيسية لاهتمامات الرقابة الداخلية وحوكمة تقنية المعلومات. وفي حين أن عمليات إدارة المشاكل والحوادث والتغيير

في آيتل ، من بين أمور أخرى، تميل إلى الدعوة إلى إنشاء إدارة كبيرة جداً لتقنية المعلومات بمستويات متعددة من الموارد البشرية والإدارية. فإنه يمكن أيضاً تطبيق هذه الممارسات المثلى الموجودة في آيتل على مؤسسة أصغر من ذلك بكثير. حيث يمكن تطبيق آيتل على جميع إدارات تقنية المعلومات بمختلف أحجامها! وحتى تكون المؤسسة متوافقة مع آيتل ، فإنها لا تحتاج إلى مستويات متعددة من موظفي الدعم، بل تحتاج إلى النظر في مختلف عمليات دعم وتقديم الخدمات من منظور أفضل الممارسات في آيتل. قد لا تحتاج إدارة صغيرة لتقنية المعلومات إلى إنشاء إدارات منفصلة لإدارة الحوادث وإدارة المشاكل مثلاً. ولكن يجب أن ننظر في كل منها على أنها عمليات منفصلة مع إجراءات رقابية فريدة ومميزة. حتى وإن كانت إدارات تقنية المعلومات في المؤسسة صغيرة جداً، فإنها ينبغي أن تُعامل كل مجال من مجالات العمليات الموجودة في آيتل على أنه مجال مستقل من أجل تحسين العمليات.

تعد البنية التحتية لتقنية المعلومات أحد المجالات الهامة لحوكمة تقنية المعلومات. في كثير من الأحيان، قد ركز كبار مديري تقنية المعلومات وغيرهم من كبار المديرين اهتمامهم على الضوابط الخاصة بالتطبيقات والضوابط العامة لتقنية المعلومات التي كانت موجودة في الماضي. أما في عالم اليوم الذي يتسم بالعمليات المعقدة التي تدعم البنية التحتية لتقنية المعلومات، فإن عمليات آيتل المبنية في هذا الفصل تصف بعض المجالات الممتازة للعناية بحوكمة تقنية المعلومات.

ملاحظة

١- كتب الآيتل متاحة من خلال مكتب المملكة المتحدة والذي يسمى مكتب المكتبة (TSO)، والذي يمكن العثور عليه في الموقع www.tsoshop.co.uk.

الفصل السابع

معايير حوكمة تقنية المعلومات: أيزو ٩٠٠١ و ٢٧٠٠٢ و ٣٨٥٠٠

في الأعوام التي تلت الحرب العالمية الثانية، برزت الولايات المتحدة زعيماً اقتصادياً وسياسياً عالمياً. وبسبب هذه الهيمنة، فقد تجاهل الكثيرون في الولايات المتحدة المعايير المتعلقة بأفضل الممارسات التجارية التي تم تطويرها واستخدامها في أماكن أخرى من اقتصادنا العالمي المترابط. إن هذه المعايير الدولية لأفضل الممارسات هي نتاج جهود تعاونية تأخذ بعين الاعتبار مجموعة واسعة من الاحتياجات والمتطلبات المحلية. إن مصدر العديد من هذه المعايير هو منظمة المقاييس والمواصفات الدولية International Standards Organization (ISO; www.iso.org) وهي هيئة يقع مقرها في جنيف بسويسرا، وقد قامت بإصدار المعايير المعتمدة والمتعارف عليها والتي تغطي مجموعة واسعة من المجالات بدءاً من المواصفات الخاصة بأسنان التثبيت الملولبة المستخدمة في محركات السيارات إلى سمك بطاقة الائتمان الشخصية ووصولاً إلى معايير الجودة الخاصة بتقنية المعلومات. وقد تم توسيع هذه المعايير على مر السنين لتشمل العديد من المجالات التي تعتبر مهمة بالنسبة لحوكمة وجودة المؤسسات.

لا بد أن يتمتع كبار المديرين التنفيذيين بمستوى فهم معين لأدوار معايير الأيزو وأي منها تناسب مؤسساتهم، كما يجب عليهم فهم المعايير الهامة بالنسبة لحوكمة فعالة لتقنية المعلومات. ويستعرض هذا الفصل ثلاثة من هذه المعايير التي تعتبر مهمة بالنسبة للممارسات الفعالة لحوكمة تقنية المعلومات. وبعد مناقشة بعض المعلومات الأساسية عن كيفية تطوير تلك المعايير الخاصة بأيزو وسبب أهميتها، فإننا سنقوم بتسليط الضوء أولاً على المعيار العالمي الذي يطلق عليه اسم أيزو ٩٠٠١ (ISO 9001)، وعلى الرغم من عدم تركيز هذا المعيار على قضايا حوكمة تقنية المعلومات على وجه الخصوص، فإن المبادئ التي جاءت في هذا المعيار قد شجعت العديد من المؤسسات على الصعيد العالمي على وضع وتنفيذ الممارسات الخاصة بجودة الإنتاج والعمليات التجارية الأخرى بصورة مستمرة.

وعلى الرغم من وجود مجموعة كبيرة من معايير الأيزو التي قد يمكن تطبيقها على حوكمة تقنية المعلومات، فإن هذا الفصل سيقوم باستعراض اثنين من تلك المعايير وبيان أهميتها وهما: أيزو ٢٧٠٠٢ (ISO 27002) وأيزو ٣٨٥٠٠ (ISO 38500). واستكمالاً لحديثنا عن اتفاقيات مستوى الخدمة SLAs التي تم تقديمها في الفصل السابع عشر من هذا الكتاب، فإن هذه المعايير تعمل على توضيح إطار العمل من أعلى إلى أسفل للقيام بتحديد ملامح عمليات إدارة الخدمات الضرورية لتقديم خدمات عالية الجودة. قد يكون فهم المعايير المناسبة لمنظمة الأيزو ISO أمراً هاماً بالنسبة لبعض الممارسات الخاصة بحوكمة تقنية المعلومات. فعلى الرغم من أن هذه المعايير يتم تطبيقها غالباً من خلال إدارة الجودة أو إحدى الإدارات بالمؤسسة، فإنه يتوجب على المدير الأول أن يكون ملماً بأهمية تلك المعايير ومجمل عمليات الأيزو.

معلومات أساسية عن معايير الأيزو:

قد يكون (مصطلح الأيزو) مربكاً بعض الشيء بالنسبة للبعض، فهو يشير إلى منظمة المقاييس والمواصفات الدولية International Standards Organization. وهي عبارة عن هيئة متخصصة في وضع المعايير العالمية، يقع مقرها في مدينة جنيف بسويسرا. وهي الجهة المسؤولة عن تطوير ونشر مجموعة واسعة من المعايير الدولية التي تتعلق بالعديد من مجالات وإجراءات الأعمال. بعض معايير الأيزو يعتبر عاماً جداً كالمعيار أيزو ١٤٠٠١ (ISO 14001)، وهو المعيار الذي يحدد المتطلبات الخاصة بالنظم الفعالة للإدارة البيئية، في حين يكون البعض الآخر منها مفصلاً ودقيقاً، كالمعيار الذي يتناول المواصفات الخاصة بحجم وسمك بطاقات الائتمان البلاستيكية. تعود أهمية المعايير الواسعة للأيزو إلى أنها تسمح لجميع المؤسسات على مستوى العالم باستخدام اللغة نفسها، وذلك عندما تصرح تلك المؤسسات بأن لديها المعيار نفسه، وليكن على سبيل المثال، معيار النظام الفعال للإدارة البيئية أيزو 14001. كما أن هناك العديد من المعايير الأكثر تفصيلاً والتي تعتبر هامة وحساسة للغاية، مثل تلك الخاصة بماكينه الصراف الآلي والموجودة في كل أنحاء العالم والتي تتوقع أن تستقبل جميعها بطاقات ائتمان لها الحجم والسمك نفسهما.

يتم تطوير معايير الأيزو من خلال تضافر جهود العديد من المنظمات الوطنية المعنية بوضع المعايير، مثل المعهد الأمريكي للمعايير الوطنية American National Standards Institute، أو غيره من المجموعات المنتشرة في جميع أنحاء العالم. تبدأ عملية وضع المعايير بشكل عام بضرورة معروفة تُحتم وجود معيار في مجال ما. مثال على ذلك معيار أيزو ٢٧٠٠١ (ISO 27001) والذي يقوم بتحديد متطلبات رفيعة المستوى لنظام فعال لإدارة أمن المعلومات. وقد تم تطوير هذا المعيار من خلال جهود اللجان الفنية الدولية التي ترعاها منظمة الأيزو بالتعاون مع اللجنة الدولية الكهروتقنية International Electrotechnical Commission، وهي إحدى الهيئات المعنية بوضع المعايير الدولية. لا يحتوي هذا المعيار على أية متطلبات تفصيلية، لكنه يحتوي على عبارات رفيعة المستوى على غرار ذكر "يجب على المؤسسة". في بعض المجالات، يتم وضع هذا النوع من الإرشادات في الإجراءات المتعلقة بعملية تدقيق تقنية المعلومات التي تم الحديث عنها في العديد من فصول هذا الكتاب.

ونظراً لمشاركة العديد من الهيئات الحكومية الدولية والمجموعات المهنية والخبراء المستقلين في عملية وضع معايير الأيزو، فإن عملية بناء واعتماد أي وثيقة من وثائق منظمة الأيزو تحتاج غالباً إلى وقت طويل. حيث تقوم لجنة من الخبراء بتطوير مسودة مبدئية للمعيار الذي يغطي مجاًلاً ما، بعد ذلك يتم إرسال تلك المسودة للمراجعة وإبداء الرأي قبل تاريخ محدد، ثم تقوم اللجنة في النهاية بمراجعة التعليقات على المسودة قبل أن تقوم بإصدار المعيار الجديد أو إرسال مسودة منقحة لإجراء جولة أخرى من المراجعات والتغييرات المقترحة. ويتم نشر معيار الأيزو عادة بعد مروره بالعديد من المراحل التي يتم من خلالها إعداد المسودات والنظر في التعليقات الخاصة بها. يمكن للمؤسسات بعد ذلك أن تقوم باتخاذ الخطوات اللازمة للامتثال لهذا المعيار. ويجب على المؤسسة أن تتعاقد مع مدقق خارجي معتمد يمتلك مهارات في هذا المعيار ليقوم بالتصديق على امتثالها لهذا المعيار.

وقد شاركت العديد من المؤسسات الأمريكية للمرة الأولى في هذه المعايير الدولية من خلال إطلاق معايير أيزو ٩٠٠٠ (ISO 9000) الخاصة بنظام إدارة الجودة في ثمانينيات

القرن الماضي، وسيتم مناقشة هذا المعيار لاحقاً في هذا الفصل. كانت الشركات الأمريكية تواجه مشاكل تنافسية بالنسبة للمنتجات التي تخضع لمعايير تصميم عالية الجودة والتي كانت مطبقة في المنتجات غير الأمريكية في ذلك الوقت مثل السيارات اليابانية. فقد قامت المؤسسات اليابانية بتصميم العديد من المنتجات العالية الجودة من خلال اتباع ما أصبح يعرف بأيزو ٩٠٠٠ (ISO 9000)، وبدأ المصنعون في الولايات المتحدة بتعديل العمليات الخاصة بهم للامتثال لهذه المعايير الخاصة بالمنتجات ذات الجودة العالية. وقد سمح هذا الامتثال بمعيار أيزو ٩٠٠٠ (ISO 9000) للمؤسسات في جميع أنحاء العالم بتصميم عملياتها التشغيلية وفقاً لمعيار واحد ثابت، ومن ثم التأكيد على أن لديهم نظاماً مُفعَلاً ومعمولاً به لإدارة الجودة وفقاً للمعيار الدولي.

تعد معايير الأيزو أكثر تحديداً وضبطاً من الإرشادات الخاصة بأفضل الممارسات مكتبة البنية التحتية لتقنية المعلومات (آيتل) والتي تناولنا الحديث عنها في الفصل السادس من هذا الكتاب. إذ يتم نشر وضبط هذه المعايير بواسطة منظمة الأيزو التي تقع في جنيف، والتي تتبع قوانين صارمة في حقوق التأليف والنشر. فالمواد الخاصة بها لا يمكن تحميلها من خلال عمليات البحث الاعتيادية على الإنترنت؛ بل لابد من شرائها. إن العديد من معايير الأيزو الفعلية عبارة عن توضيحات تفصيلية للغاية للممارسات التي يجب اتباعها.

تكون الإرشادات واضحة ولا لبس فيها ولا غموض و تشير غالباً إلى أقسام أخرى من هذا المعيار لاتباعها. تستطيع المؤسسة أن تقوم باتباع معايير منظمة الأيزو ISO والاعتماد عليها، وذلك على غرار اتباعها لأفضل الممارسات الخاصة بآيتل، إلا أن عدد معايير الأيزو أكثر بكثير من أفضل الممارسات الموصى بها في آيتل. فهي تمثل مقاييس أداء بالنسبة للمؤسسة مع نظيراتها. فمن خلال الالتزام والتمسك بتلك المعايير العالمية، يمكن للمؤسسة التحقق من أنها تعمل وفقاً لمعيار دولي ثابت، فمعايير أيزو ١٣٤٨٥ (ISO 13485) الخاصة بالمتطلبات التنظيمية لإدارة الجودة الخاصة بالأجهزة الطبية تقدم مثلاً على ذلك. حيث يحدد هذا المعيار متطلبات الجودة الخاصة بأجهزة الرعاية الصحية للإنسان، ومن الأمور الأخرى التي يتضمنها هذا المعيار، أنه يدعو المؤسسة التي تقوم بصنع مثل هذه الأجهزة إلى أن تقوم بوضع ضوابط المعايرة المناسبة. ونظراً لتنوع أساليب المعايرة، فإن المعيار لا يمكن

أن يحدد أسلوباً واحداً فحسب؛ فهو في جميع الأحوال يشترط على المؤسسات أن يكون لديها الآليات المناسبة المعمول بها.

ومن الأمور الهامة بالنسبة للمؤسسة أن تقوم بقراءة معيار الأيزو وتعديل عملياتها للتوافق معه؛ ومن الأمور الجيدة أيضاً بالنسبة للمؤسسة أن تثبت للآخرين أنها تتبع هذا المعيار. إن شهادة الأيزو هذه عبارة عن عملية مشابهة لعملية التدقيق الخارجي للسجلات المالية التي يقوم بها المحاسبون القانونيون (CPAs). فعمليات تدقيق القوائم المالية تتطلب وجود محاسب قانوني معتمد يعمل مدققاً خارجياً معتمداً لتقييم ما إذا كانت تلك التقارير المالية للمنشأة "معلنة بوضوح" وتتبع ضوابط داخلية جيدة ومعايير محاسبية معتمدة ومتعارفاً عليها أم لا. فهي تعد مفردات رفيعة المستوى، إلا أن تقريراً كهذا للتدقيق الخارجي الذي يتم التوقيع عليه مع النتائج النهائية المبلغ عنها من شأنه أن يوفر مستوى للتأكيد على أن التقارير المالية نزيهة وتستند إلى إجراءات جيدة للرقابة الداخلية.

إن عملية الحصول على شهادة الأيزو تشبه أيضاً عملية التدقيق المالي التي يقوم بها المحاسب القانوني المعتمد والذي يعتمد على التوافق مع معايير التدقيق المقبولة قبولاً عاماً (GAAS) والتي تقوم بها شركات المحاسبة العامة الكبرى. وعلى الرغم من عدم وجود الشركات "الأربعة الكبار Big4" هنا، أي مجموعة من الشركات الكبرى لتدقيق الأيزو، فإن منظمات وضع المعايير تؤهل المراجعين لأداء المراجعة الخارجية لمعايير الأيزو المختلفة. حيث لا يوجد للأيزو معايير تدقيق متعارف عليها GAAS ولكن هناك درجة كبيرة من التنوع في أهداف التدقيق، فمراجع معيار أيزو ٢٧٠٠١ (ISO 27001) الخاصة بنظم إدارة أمن المعلومات سيقوم بالبحث عن الإجراءات الرقابية المختلفة، وهذا مغاير لما سيبحث عنه مراجع معيار أيزو ١٣٤٨٥ (ISO 13485) الخاصة بنظم إدارة جودة الأجهزة الطبية. في جميع الأحوال، فإن المدقق الخارجي المؤهل لتدقيق معايير الأيزو قد يحدد الأجزاء التي تحتاج إلى إجراءات تصحيحية ويقوم بإصدار تقرير للإدارة مشابه لعمليات التدقيق الداخلي، كما سيتم مناقشته في الفصل التاسع عشر من هذا الكتاب. وبمجرد أن يتم تصحيح توصيات مدقق الأيزو، فإن المراجع الخارجي سوف يشهد بأن المؤسسة متوافقة مع المعيار.

وبمجرد اعتماد المؤسسة، فإنها تستطيع أن تعلن للعالم الخارجي أن العمليات المتبعة لديها تُلبّي ذلك المعيار الخاص بالأيزو. على سبيل المثال، فإن أحد الزبائن الذين يتعاملون مع أجهزة التشخيص الطبي يريد أن يعرف ما إذا كان المورد المحتمل متوافقاً مع معيار أيزو ١٣٤٨٥ (ISO 13485) أم لا. وإن هذا المصنّع للجهاز الطبي نفسه سيرغب أيضاً في الحصول على ضمانات بأن موردي المكونات الأولية لها مؤهلون من قبل الأيزو. وعلى الرغم من وجود مجموعة كبيرة من معايير الأيزو، فإن الأقسام التالية تستعرض عدداً من المعايير التي لها أهمية بالنسبة للضوابط الداخلية والحوكمة والتي تشهد نمواً متزايداً على مستوى العالم في الوقت الراهن.

معايير الأيزو ٩٠٠٠ لإدارة الجودة:

تمتلك معايير الأيزو ٩٠٠٠ (ISO 9000) تراثاً يعود تاريخه إلى أيام الحرب العالمية الثانية. وذلك عندما كان طرفا الصراع بحاجة إلى توحيد قوي لمواصفات المنتجات أثناء القيام بإنتاج العديد منها. حتى وإن كانت هذه المنتجات عبارة عن الرصاص والقنابل، كان يجب عليهم العمل بشكل صحيح لتوحيدها. فقد كانت هناك حاجة لفرض رقابة صارمة على جودة المنتجات. وظهرت بعض الإجراءات القياسية القوية من جانب الحلفاء الغربيين لضمان الجودة، كما ظهرت مهن كالمهندسين الصناعيين وأخصائيين للعمل في مراقبة جودة الإنتاج. وبعد انتهاء الحرب، تم إنشاء منظمة الأيزو على أنها جزء من الاتفاقية العامة للتجارة والتعريفات الجمركية (General Agreement on Trade and Tariffs (GATT) أو ما يعرف باسم (اتفاقية الجات). وهي إحدى الاتفاقيات الدولية الهادفة إلى جعل العالم يعيش في بيئة أكثر أمناً. كانت معايير الأيزو ٩٠٠٠ الخاصة بنظم إدارة الجودة واحدة من المعايير الأولى التي أصدرتها منظمة الأيزو. وقد لاقت الاهتمام الأول بها والأكبر من قبل البلدان الأوروبية التي كانت تتعافى حديثاً من آثار الحرب.

وقد كانت اليابان واحدة من البلدان التي بحاجة إلى إعادة الإعمار والتعافي من الحروب، وهي البلد التي قامت بتبني نظم إدارة الجودة بشدة في تلك الفترة. وقد قام اليابانيون في خمسينيات وستينيات القرن الماضي بتوجيه دعوة لعدد من خبراء أنظمة الجودة الأمريكيين مثل ديلو إدواردز ديمينج^(١)، W. Edwards Deming، وآخرين ليقوموا بمد يد العون

والمساعدة لهم في العديد من المصانع اليابانية. وفي الوقت الذي تم فيه تجاهل هؤلاء الخبراء إلى حد ما في الولايات المتحدة، قامت الصناعة اليابانية بتبني فلسفتهم وتقنياتهم بشكل كبير وملحوظ. وبحلول منتصف السبعينيات من القرن الماضي بدأت الشركات اليابانية المصنعة للإلكترونيات والسيارات تشق طريقها بشكل كبير في أسواق الولايات المتحدة نظراً لجودة وقيمة منتجاتها. وقد بدأ الكثيرون في الولايات المتحدة في إدراك أن هذه المنتجات اليابانية الصنع قد تفوقت على منتجاتهم في كثير من النواحي. فقد أصبحت معايير الجودة الخاصة بالأيزو (ISO 9000) عاملاً ذا أهمية متزايدة في قياس وتقييم جودة المنتجات في جميع أنحاء العالم.

إن الأيزو ٩٠٠٠ (ISO 9000) هي عبارة عن عائلة من المعايير الخاصة بنظم إدارة الجودة والتي يتم تنظيمها وصياغتها من قبل منظمة الأيزو. وتتضمن هذه المعايير متطلبات لأمر مثل:

- مراقبة العمليات لضمان أنها فعالة.
- حفظ سجلات وافية عن إجراءات العمل.
- فحص مخرجات الإنتاج من أجل اكتشاف العيوب، مع بدء الإجراءات التصحيحية المناسبة عند الضرورة.
- مراجعة منتظمة للعمليات الفردية ونظام الجودة الشاملة من أجل الفاعلية.
- تسهيل عمليات التحسين المستمر.

يشير كل بند من هذه البنود إلى مجموعة من العمليات، لا إلى إجراءات معينة. ولكي تثبت مؤسسة ما أنها متوافقة على سبيل المثال مع الأيزو ٩٠٠٠ (بالتحديد معيار أيزو ٩٠٠١) - والذي يقوم بمتابعة العمليات الرئيسية لتكون أكثر فاعلية، فإنه يتوجب عليها في كثير من الأحيان أن تقوم بعمل العديد من التغييرات في إجراءاتها الإدارية ووثائقها الداعمة. إن الامتثال بأحد معايير الأيزو يخلق أيضاً مستوى مطلوباً من التوقعات. فعندما تحصل المؤسسة في أي مكان في العالم على مثل هذه المعايير، فهي بذلك تعلن أنها تمتلك أنظمة فعالة ومعمولاً بها لإدارة الجودة. إن المؤسسة التي يتم تدقيقها واعتمادها بشكل مستقل

لتكون متوافقة مع أيزو ٩٠٠١ على سبيل المثال، قد تعلن صراحة أنها "معتمدة من الأيزو ٩٠٠١" أو "مسجلة لدى الأيزو ٩٠٠١". لا تضمن شهادة معيار أيزو ٩٠٠١ الامتثال (ومن ثم الجودة) للمنتجات والخدمات النهائية، وإنما هي فقط شهادة تدل على أنه يتم تطبيق العمليات التجارية والإنتاجية الملائمة.

تتم عملية الاعتماد الفعلية من خلال الفحص الذي يقوم به أحد المدققين المعتمدين في الأيزو والمتخصصين في معيار محدد من معاييرها. وكما تحدثنا سابقاً فإن هذه العملية تشبه عملية المراجعة والتدقيق التي يقوم بها المحاسبون القانونيون (CPAs) لاعتماد القوائم المالية الخاصة بإحدى المؤسسات. وبالتنسيق مع منظمات المعايير الوطنية لديهم يتم التفويض والسماح لمدققي الأيزو بتسجيل امتثال المؤسسة لمعيار فريد من معايير الأيزو.

إن معايير الأيزو ٩٠٠٠ وغيرها من المعايير الأخرى للأيزو تفرض على المؤسسة متطلبات توثيقية ضخمة، فلا يكفي أن تدعي المؤسسة بأنها قامت بتوثيق عملية ما لمرة واحدة فقط. بل يجب أن تكون هناك عملية مستمرة لإبقاء هذا التوثيق فعالاً ومستمرًا. في السنوات الماضية، بذلت العديد من المؤسسات الجهود لتوثيق إحدى المبادرات أو العمليات الجديدة للمرة الأولى ولكنها فشلت في المحافظة على هذا التوثيق. وقد تعرض العديد من مدققي تقنية المعلومات لمثل هذه الحالات. فكثيراً ما كانوا يسألون عما إذا كان قد تم توثيق النظام أو العملية التي هم بصدد مراجعتها حالياً، وفي حال كانت الوثائق غير محدثة أو غير موجودة، فإن هذا القصور سيظهر غالباً في نتائج التقرير الخاص بعملية التدقيق، وفي كثير من الأحيان لا يؤدي ذلك إلا إلى القليل من الإجراءات التصحيحية النهائية. إن الامتثال لمعايير الأيزو ٩٠٠٠ يرفع سقف المتطلبات الخاصة بعمليات الجودة إلى مستوى جديد كلياً. لذا يجب على مراجع الأيزو أن يصدق أو يشهد على امتثال المؤسسة بالمعيار لكي تتمكن من الإعلان للعالم الخارجي بأنها متوافقة مع معيار الأيزو.

إن الأيزو ٩٠٠٠ هو عبارة عن مجموعة من المعايير الخاصة بنظام الجودة القائم على التحسين المستمر، سواء كان ذلك لإحدى المنتجات الصناعية أم العمليات الخدمائية. يوضح الشكل التوضيحي (٧-١) تلك العملية الخاصة بنظام إدارة الجودة التي تقودها سلسلة من الإجراءات الداخلية لتحسينات المستمرة وطلبات العملاء أيضاً. في هذه العملية المستمرة،

يجب مراقبة العمليات الموجودة والإجراءات المخطط لها لإدخال التحسينات وعناصر الإجراءات التي يتم تنفيذها لعمليات المراقبة، وإدخال المزيد من التحسينات المستقبلية. لا تعد عملية التحسين المستمر للجودة من العمليات الجديدة بالنسبة للعديد من كبار المديرين. فقد قام محترفو تطوير نظم تقنية المعلومات بالأساس باستخدام المجموعة نفسها من العمليات العامة التي كانت موجودة منذ الأيام الأولى لتطوير النظم التقنية في عملية تطوير النظم الجديدة في تقنية المعلومات والتي تدعى دورة حياة تطوير النظم SDLC. وقد دعت تلك التطبيقات التي تم تطويرها باستخدام أسلوب عملية دورة حياة تطوير النظم SDLC إلى قدر كبير من الوثائق التي كانت في أغلب الأحيان غير جاهزة. أما اليوم فيتم تطوير تطبيقات تقنية المعلومات من خلال عمليات غير رسمية ودورية وسريعة بشكل أكبر لتطوير التطبيقات.

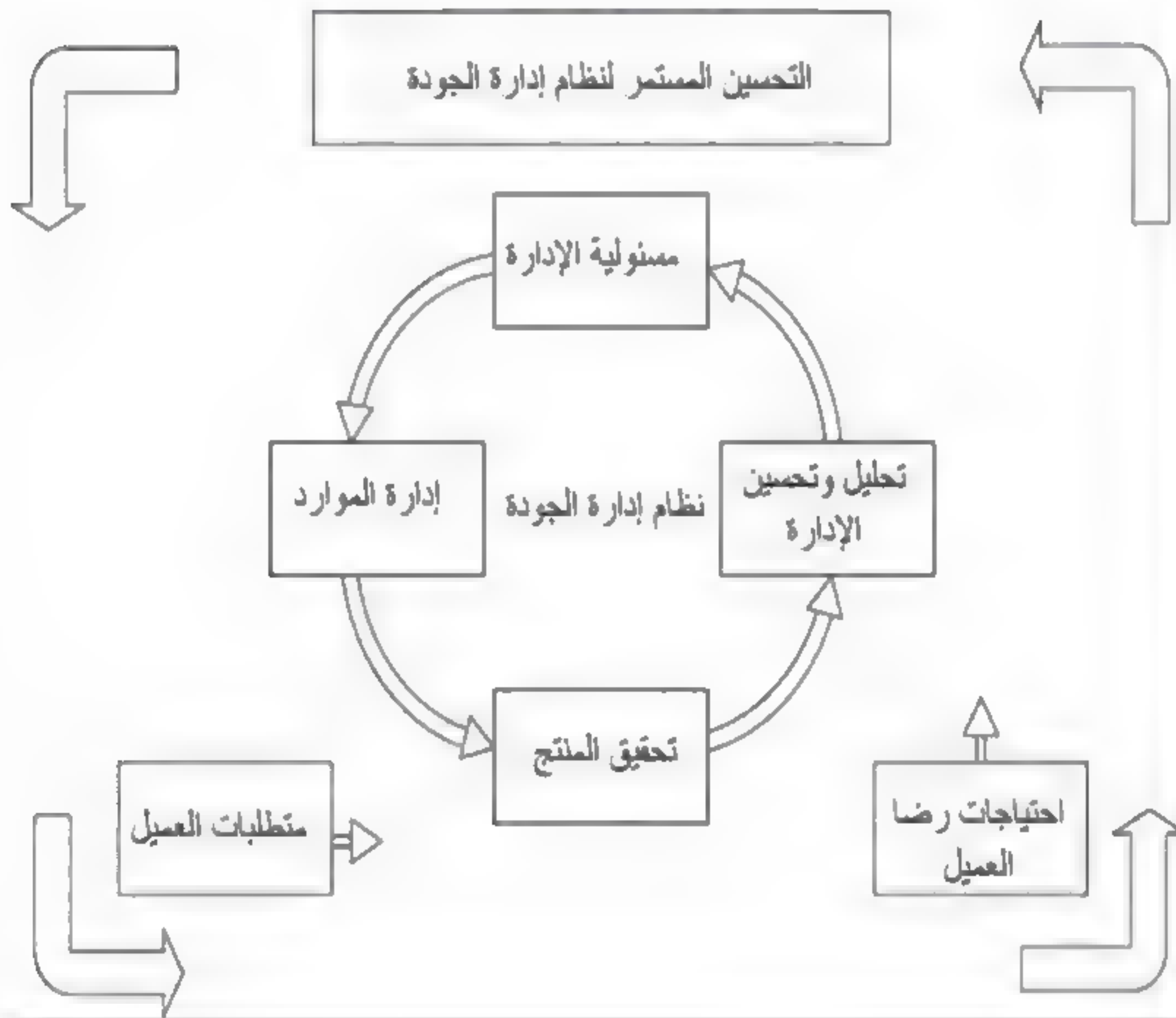
إن التوثيق الصارم والدقيق مهم جداً بالنسبة للمؤسسة التي تسعى للتسجيل في الأيزو، وهو مطلب عالمي. حيث تدعو أفضل الممارسات في الأيزو إلى اتباع التسلسل الهرمي للتوثيق في أي مجال، بدءاً من الإرشادات الرفيعة المستوى التي توضح أسباب الممارسة، وصولاً إلى التعليمات التفصيلية التي توضح الكيفيات التي تتم من خلالها الممارسة. الشكل التوضيحي (٧-٢) يعرض هذا التسلسل الهرمي للتوثيق حيث تم وضع "النماذج والوثائق" في الجزء السفلي من المثلث، والتي تعمل على توفير الأدلة والبراهين. فهذا التوثيق ضروري وأساسي لدعم نظام إدارة الجودة، ومن المؤكد أنه يُطلب من قبل مدققي التصديق الخارجين للأيزو.

لقد وفر هذا القسم وصفاً رفيع المستوى جداً لمعايير الأيزو ٩٠٠٠ الخاصة بعملية إدارة الجودة. ومع ذلك، قد يتساءل القارئ: "لماذا يجب عليّ الاهتمام بالأيزو، وما الذي لديها لتقدمه لحوكمة تقنية المعلومات؟" نقول، إن التوافق مع هذه العمليات الخاصة بالأيزو ٩٠٠٠ مهم بالنسبة لجميع أنواع المؤسسات لتعلن للإدارة الداخلية الخاصة بها وللعمام الخارجي بأنها تركز على الجودة. ومثال على ذلك، في عام ١٩٩٥ أصبح المعهد الأمريكي للمحاسبين القانونيين أول منظمة مهنية عالمية كبرى معتمدة وحاصلة على شهادة الأيزو ٩٠٠١^(٣). فمن الواجب أن تقوم جميع المنظمات على مختلف المستويات

بالنظر في تبني عمليات الأيزو ٩٠٠٠. فكثير من الإعلانات الموجودة اليوم لكثير من المنتجات أو الخدمات المعروضة تصرح أو تذكر أن البائع حاصل على شهادة الجودة ومعتمد من قبل منظمة الأيزو، ويستطيع أي عميل طلب المزيد من المعلومات التي تتعلق بمستوى هذه الشهادة قبل أن يقرر إتمام عملية الشراء.

شكل توضيحي (١-٧)

عملية نظام إدارة الجودة



تحدد معايير الأيزو بعض أفضل الممارسات الرفيعة في العديد من مجالات العمليات التشغيلية لتقنية المعلومات. حتى وإن كانت المؤسسة لا تسير بنسبة مئة في المئة في استكمال جميع المتطلبات الخاصة بأحد معايير الأيزو وتكمل متطلبات التدقيق الخاصة بالأيزو، فإن المعايير سوف توفر بعض الإرشادات القوية والمثبتة لبناء عمليات داخلية قوية.

تناقش الأقسام التالية بمزيد من التفصيل المتطلبات الخاصة باثنين من هذه المعايير التي تعتبر مهمة بالنسبة للعمليات الفعالة لحوكمة تقنية المعلومات.

شكل توضيحي (٧-٢)

هرمية الوثائق في الأيزو



معايير الأيزو الخاصة بأمن تقنية المعلومات: أيزو ٢٧٠٠٢ و ٢٧٠٠١:

إن أيزو ٢٧٠٠٢ (ISO 27002) هو عبارة عن معيار هام في النواحي الأمنية المرتبطة بتقنية المعلومات، ومصمم لمساعدة أي مؤسسة تحتاج إلى وضع برنامج شامل لإدارة أمن المعلومات أو تحسين ممارساتها الحالية المتعلقة بأمن المعلومات. وبعيداً عن موضوعات الحوكمة وأمن تقنية المعلومات التي نُوقشت في الفصل العاشر من هذا الكتاب، فإن أيزو ٢٧٠٠٢ يعد أحد المعايير التي تخص طائفة عريضة من مصادر المعلومات وأمن المعلومات بشكل عام. ولأن هناك العديد من الأشكال التي يمكن أن تتواجد بها مثل هذه البيانات، فإن المعيار يأخذ نهجاً موسعاً ويحتوي على مجموعة كبيرة من المعايير الأمنية التي تتعلق بالتالي:

- الملفات الإلكترونية للبيانات والبرمجيات.
 - جميع أشكال المستندات الورقية، متضمناً ذلك المواد المطبوعة والملاحظات المكتوبة بخط اليد والصور.
 - تسجيلات الفيديو والتسجيلات الصوتية.
 - المحادثات الهاتفية وكذلك البريد الإلكتروني والفاكس والفيديو وغيرها من أشكال الرسائل.
- الفكرة هنا هي أن المعلومات بجميع أشكالها لها قيمة وبحاجة إلى حماية، تماماً كأى أصل من الأصول الأخرى الموجودة في الشركة. إن العديد من المؤسسات اليوم لا تضع حتى تلك المعايير الأمنية في الحسبان فيما يتعلق بتلك المجالات الواسعة، لكن معيار أيزو يشير إلى أنه لا بد من تضمين هذه المعايير الأمنية قدر المستطاع. كما يقترح أيضاً ضرورة حماية البنية التحتية التي تدعم هذه المعلومات، والتي تتضمن الشبكات والنظم والوظائف من مجموعة واسعة من التهديدات. والتي تتضمن أي شيء ابتداءً من الأخطاء البشرية وتعطل المعدات إلى أن يصل إلى السرقة والاحتيال والأعمال التخريبية من خارج المؤسسة والتخريب المتعمد من قبل العاملين في المؤسسة والحريق والفيضانات وحتى الإرهاب.
- وعلى غرار جميع المعايير الأخرى لمنظمة الأيزو. فإن هذا المعيار المنشور لا يقوم حقيقة بوصف ما هو المطلوب على وجه التحديد، لكنه يحدد المجالات التي تحتاج إلى معايير تتعلق بالأمن. الشكل التوضيحي (٧-٣) يوضح الموضوعات الرئيسية لمعيار أيزو ٢٧٠٠٢. فالمعيار لا يحتوي على المتطلبات التفصيلية لكل من هذه المجالات - فالمعيار الدولي الشامل والثابت يتطلب نصاً شاملاً ومكثفاً ولكن لن يكون شاملاً للجميع، وقد يصبح غير صالح. فبدلاً من ذلك على سبيل المثال. يدعو السطر (٤-٢) إلى المعايير الأمنية الخاصة بسياسات وصول الشريك الخارجي أو ما يسمى الطرف الثالث Third Party للبيانات. فالأيزو يدعو إلى أن يكون لدى المؤسسة عمليات موثقة ومعتمدة تشمل السياسات التي تحكم وصول الشريك الخارجي أو الطرف الثالث إلى البيانات والنظم. لذا يجب على المنشأة أن تضع معايير وإجراءات أكثر تفصيلاً خاصة بها في هذا المجال. إن نوع ومدى هذه المعايير يمكن أن يعتمد على عوامل كثيرة. لذا يجب أن تقوم المؤسسة الممثلة لمعيار الأيزو ٢٧٠٠٢ بمعالجة هذه القضية جنباً إلى جنب مع المجالات الأخرى في المعيار.

الشكل التوضيحي (٣-٧)

مجالات موضوع معايير الأيزو ٢٧٠٠٢

يسرد هذا الملخص مجالات الموضوعات الرفيعة المستوى الموجودة في هذا المعيار الصادر من منظمة الأيزو (ISO 27002). الخطوط العريضة الفعلية للمعيار تنخفض إلى مستويات متعددة، وأكثر تفصيلاً لكل نقطة من النقاط. هذا المستوى من المخطط التفصيلي يعتبر نموذجاً لجميع معايير الأيزو.

- ١- النطاق: وصف رفيع المستوى لتطبيق هذا المعيار.
- ٢- المصطلحات والتعريفات: بما يتفق مع معايير الأيزو الأخرى فإن المصطلحات الرئيسية كافة يتم تعريفها (على سبيل المثال، تعريف المقصود بـ "السرية").
- ٣- المعايير أو الحاجة إلى سياسة عالية المستوى لأمن المعلومات.
- ٤- المتطلبات اللازمة للإدارة الأمنية في المؤسسة:
 - ٤-١ البنية التحتية لأمن المعلومات.
 - ٤-٢ السياسات الأمنية ووصول الطرف الثالث.
 - ٤-٣ اعتبارات الاستعانة بمصادر خارجية (اعتبارات التعاقد الخارجي).
 - ٥- معايير تصنيف الأصول والرقابة:
 - ٥-١ المساءلة عن الأصول.
 - ٥-٢ تصنيفات المعلومات.
 - ٦- أمن الأفراد:
 - ٦-١ الاعتبارات الأمنية في تعريفات الوظيفة والموارد.
 - ٦-٢ تدريب المستخدم على أمن الأفراد.
 - ٦-٣ معايير الاستجابة للحوادث الأمنية والأعطال.

٧- الأمن المادي والبيئي، متضمناً ذلك متطلبات لـ:

١-٧ المناطق الآمنة.

٢-٧ أمن المعدات.

٣-٧ الضوابط العامة.

٨- إدارة الاتصالات وعمليات التشغيل:

١-٨ الإجراءات التشغيلية والمسؤولية.

٢-٨ التخطيط والموافقة على النظام.

٣-٨ الحماية ضد البرمجيات الخبيثة.

٤-٨ إدارة الممتلكات.

٥-٨ متطلبات إدارة الشبكة.

٦-٨ معالجة الوسائط والأمن.

٧-٨ تبادل المعلومات والبرمجيات.

٩- التحكم في الوصول:

١-٩ متطلبات الأعمال للتحكم في الوصول.

٢-٩ إدارة الوصول للمستخدم.

٣-٩ مسؤوليات المستخدم بالنسبة للمعايير الأمنية.

٤-٩ التحكم في الوصول إلى الشبكة.

٥-٩ التحكم في الوصول لنظام التشغيل.

٦-٩ إدارة الوصول للتطبيقات.

٧-٩ معايير المراقبة للوصول إلى النظام واستخدامه.

٨-٩ الحوسبة المتنقلة والشبكات ذات الصلة.

١٠- معايير تطوير النظام وصيانته:

١٠-١ المتطلبات الأمنية للأجهزة ونظم البرمجيات.

١٠-٢ أمن نظم التطبيقات.

١٠-٣ ضوابط التشفير.

١٠-٤ أمن ملفات النظام.

١٠-٥ الأمن في عمليات التطوير والدعم.

١١- معايير إدارة استمرارية العمل.

١٢- المعايير الأمنية التي تغطي قضايا الامتثال:

١٢-١ الالتزام بالمتطلبات القانونية.

١٢-٢ مراجعات السياسة الأمنية والتوافق الفني.

١٢-٣ اعتبارات تدقيق النظم.

في خطوة أولى لتطبيق معيار أيزو ٢٧٠٠٢، فإنه يجب على المؤسسة أن تقوم بتحديد احتياجات ومتطلبات أمن المعلومات الخاصة بها. وهذا يتطلب القيام بإجراء تقييم لمخاطر أمن المعلومات على غرار عمليات إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية (COSO)، والتي تم الحديث عنها في الفصل الرابع من هذا الكتاب. يجب أن يركز مثل هذا التقييم على تحديد التهديدات والثغرات الأمنية إلى جانب تحديد الكيفية التي من خلالها يمكن اعتبار كل واحد منها سبباً محتملاً في وقوع الحوادث الأمنية. وينبغي أن تساعد هذه العملية على تحديد الاحتياجات والمتطلبات الفريدة لأمن المعلومات في المؤسسة.

لوضع عمليات خاصة بفرض معيار الأيزو ٢٧٠٠٢ الخاص بأمن المعلومات ينبغي على المؤسسة أن تقوم بتحديد وفهم جميع المتطلبات القانونية والتشريعية والتنظيمية

والتعاقدية التي يجب أن تفي بها المؤسسة ويفي بها أيضاً الشركاء التجاريون والمقاولون ومقدمو الخدمات الذين تتعامل معهم المؤسسة. ويحتاج ذلك إلى فهم وتحديد الاحتياجات والمتطلبات الأمنية الخاصة بالمؤسسة.

يعد أيزو ٢٧٠٠٢ المعيار الأول من بين سلسلة من المعايير الدولية المستهدفة من قبل المؤسسات التي تستخدم نظم الحاسب الآلي الداخلية أو الخارجية، أو التي تمتلك بيانات سرية أو تعتمد على تقنية المعلومات لتنفيذ أنشطة الأعمال الخاصة بها، أو التي ترغب ببساطة في اعتماد مستوى أعلى من الأمان عن طريق التوافق مع المعيار. وتماماً كما أصبح الامتثال لمعايير الأيزو ٩٠٠٠ بمثابة ضمان الجودة، فإن التوافق مع معيار أيزو ٢٧٠٠٢ يُمكن الشركاء من أن يكونوا على ثقة في مجمل العمليات الأمنية في المؤسسة. لا بد أن يسهم الامتثال بمعيار أيزو ٢٧٠٠٢ في تعزيز مستوى الثقة المتبادلة بين الشركاء، حيث يمكن لكل منهم إثبات أنه يتبع المعايير الأمنية المتوافقة مع مجموعة من المعايير المعترف بها والمعتمدة عالمياً. عندما يزداد نطاق الامتثال لمعيار أيزو ٢٧٠٠٢ ويصبح أكثر شمولاً وانتشاراً، فمن الممكن أن يسهم ذلك في انخفاض أقساط التأمين ضد مخاطر الحاسب الآلي، إلا أنه من المؤكد سيوفر مستوى حماية أفضل للبيانات السرية ويحسن من ممارسات الخصوصية والامتثال لقوانين الخصوصية. يعد معيار أيزو ٢٧٠٠٢ منهجية منظمة ومعترفاً بها دولياً تساعد المؤسسة على تطوير إدارة أفضل لأمن المعلومات بصفة مستمرة.

ودعماً لهذا المستوى الرفيع للمعيار الخاص بالضوابط الأمنية، فإن معيار أيزو ٢٧٠٠١ (ISO 27001) وهو ما تعرفه منظمة الأيزو على أنه "مواصفة" خاصة بنظام إدارة أمن تقنية المعلومات. بمعنى أنه قد تم تصميم هذا المعيار لقياس ومراقبة وضبط إدارة الأمن من منظور من أعلى إلى أسفل، إلا أن المعيار أيزو 27001 يوضح كيفية تطبيق معيار أيزو 27002 ويوضح بأن عملية تطبيق هذا المعيار الخاص بأمن المعلومات تتكون من ستة أجزاء:

١- تحديد السياسة الأمنية: ثمة عنصر أساسي في أي معيار هو الحاجة إلى بيان بالسياسة الرسمية معتمد من قبل الإدارة العليا. وسيتم قياس جميع جوانب التوافق الأخرى للمعيار مقابل هذا البيان الخاص بالسياسة.

٢- تحديد نطاق نظام إدارة أمن تقنية المعلومات IT security management system (ITSMS):

يعرف معيار أيزو ٢٧٠٠٢ الأمن بعبارات فضفاضة قد لا تناسب أو لا تحتاج إليها جميع المؤسسات. فبعد أن قمنا بتعريف السياسة الأمنية رفيعة المستوى فإن المؤسسة تحتاج إلى تحديد نطاق نظام إدارة أمن تقنية المعلومات IT security management system (ITSMS) النشاط الخاص بها. على سبيل المثال، يحدد معيار أيزو ٢٧٠٠٢ عنصراً من عناصر المتطلبات الأمنية كتسجيلات الفيديو والصوت. وقد لا يكون هذا ضرورياً لمؤسسة معينة، ومن ثم سيتم تحديد استبعادها فيما يتعلق بنطاق نظام إدارة أمن تقنية المعلومات (ITSMS) الخاص بها.

٣- إجراء تقييم المخاطر: ينبغي على المؤسسة أن تحدد منهجية لتقييم المخاطر تناسب بيئة ITSMS الخاصة بها، وبعد ذلك تقوم بوضع معايير لقبول المخاطر وتحديد ما يمكن أن يشكل مستويات مقبولة من المخاطر.

٤- إدارة المخاطر: تعد هذه إحدى العمليات الرئيسية التي تشمل التحديد الرسمي للمخاطر وتحليل المخاطر وخيارات لمعالجة تلك المخاطر. وهذا العنصر الأخير يمكن أن يشمل تطبيق الضوابط المناسبة لتجنب المخاطر وقبول المخاطر واتخاذ خطوات أخرى لتجنبها، أو نقل المخاطر إلى أطراف أخرى مثل شركات التأمين أو الموردين.

٥- اختيار أهداف الرقابة والضوابط التي سيتم تنفيذها: تعد هذه الخطوة مشابهة جداً لإجراءات الرقابة الداخلية للإطار (COSO) والتي تمت مناقشتها في الفصل الرابع من هذا الكتاب وكذلك عمليات الرقابة الداخلية في (كوبت) التي نوقشت في الفصل الخامس من هذا الكتاب أيضاً. فلكل هدف من الأهداف الرقابية المعرفة، يجب على المؤسسة أن تحدد الإجراءات الرقابية المناسبة له.

٦- إعداد بيان الانطباق: تعد هذه الوثائق الرسمية ضرورية لإنهاء عملية توثيق ITSMS. فمثل هذه الوثائق هي التي تطابق أهداف الرقابة مع الإجراءات الخاصة بإدارة وتنفيذ ITSMS.

وكما هو واضح من هذه الخطوات الست، فإن عملية تحليل المخاطر وتحديد السياسات الأمنية المتبعة يعد من الأمور الرئيسية الهامة بالنسبة لهذا المعيار الخاص بتقنية المعلومات. ونظراً للقواعد الصارمة في حقوق النشر والتأليف الخاصة بالأيزو، فإننا لم نتمكن من إدراج مقاطع محددة من معيار أيزو ٢٧٠٠١ في هذا الفصل. يتم عرض المعايير الفعلية للأيزو في نص محكم واضح لا لبس فيه. ويتم إضافة القليل من التفاصيل المحددة، إلا أن هناك ما يكفي للسماح للمؤسسة بتطبيق النظام الخاص بها لإدارة أمن تقنية المعلومات ITSMS. ويتم اختتام كل معيار بملحق يسرد إجراءات الرقابة الخاصة بتفاصيل كل هدف من أهداف هذا المعيار. ومع ذلك، لا ينبغي النظر إلى معيار أيزو ٢٧٠٠١ على أنه مجموعة شاملة من الإجراءات الرقابية التي سيتم تغييرها بمجرد تغيير التقنية، وإنما هي عبارة عن خطوط عريضة للإطار الخاص بنظام إدارة أمن تقنية المعلومات ITSMS والتي ينبغي تنفيذها ومراقبتها، وصيانتها باستمرار.

يعتبر كل من أيزو ٢٧٠٠١ وأيزو ٢٧٠٠٢ معايير عالمية تحتوي على مخططات جاهزة ومتعارف عليها للامتثال بها والحصول على شهادتها، خاصة في المملكة المتحدة والاتحاد الأوروبي. وسيستمر كل منها في التطور ومواكبة التقنية والتوسع تبعاً للتغيرات الأكثر شمولية. وتقوم هذه المعايير أيضاً بتوفير الأساس اللازم لتحديد المعايير والممارسات الفعالة في أمن تقنية المعلومات.

معيار أيزو ٣٨٥٠٠ الخاص بحوكمة تقنية المعلومات:

يتم تطوير معايير الأيزو ومن ثم إصدارها في المجالات التي تحتاج بشكل واضح إلى إرشادات تتعلق بأفضل الممارسات الموجودة على المستوى العالمي. في بعض الأحيان يتم إصدار هذه المعايير عندما يكون هناك حاجة تجارية ماسة لتوحيد المواصفات القياسية لمنتج ما. فمعيار أيزو الذي قمنا بالإشارة إليه مسبقاً والذي يتناول موضوع حجم بطاقات الدفع الائتمانية الخاصة بالعميل يعد مثلاً على ذلك. فقد قام مقدمو البطاقات الائتمانية في الأيام الأولى لها بإصدار بطاقات ذات أحجام وأنظمة ترقيم ومواصفات أخرى مختلفة. وبالمثل فقد كانت هناك حاجة إلى معايير خاصة بالعمليات التبادلية لتعزيز التجارة الإلكترونية، وبناء على ذلك تم إطلاق أحد معايير الأيزو الخاصة بهذا الشأن. في بعض

الحالات الأخرى تمثل معايير الأيزو أفضل الممارسات عندما يكون الامتثال بها ضرورياً لأغراض تجارية. ولعل حديثنا السابق عن معايير الأيزو ٩٠٠٠ الخاصة بالجودة هو خير مثال على ذلك. تقريباً كل مؤسسات تصنيع المنتجات اليوم التي ترغب في المنافسة على الصعيد الدولي يجب أن يكون مشهوداً لها بالتوافق مع معايير الأيزو ٩٠٠٠ الخاصة بنظام إدارة الجودة.

على الرغم من أن بعض معايير الأيزو ظلت معمولاً بها لسنوات عديدة. فإن معيار أيزو ٣٨٥٠٠ الخاص بحوكمة تقنية المعلومات يعتبر جديداً نسبياً، وقد تم إطلاقه في عام ٢٠٠٨ بعد فترة طويلة من التطوير. كما أنه لم يلق في الوقت الحاضر مستوى جيداً من الاهتمام الدولي، على الرغم من أن الإصدارات الجديدة المخطط لها للإطار كوبت، والذي تم الحديث عنه في الفصل الخامس من هذا الكتاب سوف تضم المبادئ الخاصة بمعيار أيزو ٣٨٥٠٠. فبالإضافة إلى إطار الرقابة الداخلية (COSO)، الذي تم الحديث عنه في الفصل الرابع من هذا الكتاب، والإطار كوبت، والذي تناولنا الحديث عنه في الفصل الخامس من هذا الكتاب، وأفضل الممارسات للإطار آيتل الذي تحدثنا عنه في الفصل السادس من هذا الكتاب؛ فإن معيار أيزو ٣٨٥٠٠ يعد إطاراً آخر للمساعدة في دعم الممارسات الفعالة لحوكمة تقنية المعلومات الخاصة بمؤسسة ما. حتى الآن تم إطلاق المعيار على مستوى عالٍ جداً، أما الأجزاء والإرشادات التفصيلية فمن المؤكد أنها ستأتي لاحقاً. يقدم هذا القسم وصفاً لمعيار أيزو ٣٨٥٠٠ وكيف يمكن أن يساعد المؤسسة على وضع ممارسات فعالة لحوكمة تقنية المعلومات.

أهداف معيار أيزو ٣٨٥٠٠:

يوفر هذا المعيار إطاراً من المبادئ الخاصة بكبار المديرين لاستخدامها عند تقييم وتوجيه ومراقبة استخدام تقنية المعلومات في مؤسساتهم. وهذا من شأنه أن يساعدهم على فهم الالتزامات القانونية والتنظيمية والأخلاقية المتعلقة باستخدام مؤسساتهم لتقنية المعلومات والوفاء بها. ويضم الإطار نموذجاً للتعريفات والمبادئ والحوكمة ليحقق ثلاثة أهداف هي:

- ١- توفير ضمانات لجميع أصحاب المصلحة في المؤسسة في أن يكون لديهم ثقة في حوكمة الشركات في الأمور التي تتعلق بتقنية المعلومات في مؤسساتهم.
- ٢- إعلام وتوجيه كبار المديرين للتحكم في استخدام تقنية المعلومات في منظماتهم.
- ٣- توفير أساس لتقييم أهداف حوكمة الشركات فيما يخص تقنية المعلومات.

كما يهدف معيار أيزو ٣٨٥٠٠ إلى إرشاد أولئك المشاركين في تصميم وتنفيذ نظم الإدارة العليا الخاصة بالسياسات والعمليات الفعالة التي تدعم حوكمة تقنية المعلومات. بمعنى أنه، بينما تشير إرشادات هذا المعيار أكثر إلى مستويات الإدارة العليا، فإنه ينبغي على جميع المهنيين المشاركين في تصميم أو تنفيذ أو إدارة أو مراجعة عمليات تقنية المعلومات إعطاء بعض الاهتمام لمثل هذه المعايير الواسعة النطاق.

يُطبق هذا المعيار على حوكمة عمليات إدارة تقنية المعلومات وقراراتها التي يتم التحكم فيها إما من قبل المتخصصين في تقنية المعلومات داخل المنظمة، أو من قبل مقدمي الخدمات الخارجيين، أو من قبل وحدات العمل الأخرى في المؤسسة. يهدف المعيار إلى تقديم دليل إرشادي للمتخصصين في تقنية المعلومات ليقوموا بتقديم المشورة أو تقديم المعلومات أو مساعدة كبار المسؤولين التنفيذيين، مثل:

- كبار المديرين.
- أعضاء المجموعات التي تقوم بمراقبة الموارد داخل المنظمة.
- أخصائيي العمل الخارجي أو التقني مثل القانوني أو المحاسبي.
- الأخصائيين، أو جمعيات تجار التجزئة، أو الهيئات المهنية.
- بائعي الأجهزة والبرمجيات والاتصالات وغيرها من منتجات تقنية المعلومات.
- مقدمي الخدمات الداخليين والخارجيين (متضمناً ذلك استشاريي تقنية المعلومات).
- مدققي تقنية المعلومات.

إن النطاق والأهداف المشار إليها تكون كبيرة إلى حد ما بالنسبة لمعيار جديد وصغير نسبياً. ومع ذلك، هناك بعض المبادئ العامة الرئيسية التي تم وضعها في النص الحالي

الخاص بها، ويمكننا أن نتوقع أن نرى تعريفات دعم وإرشادات أكثر تفصيلاً لمعيار أيزو ٣٨٥٠٠ في السنوات المقبلة.

إطار عمل معيار أيزو ٣٨٥٠٠ لحوكمة تقنية المعلومات:

يحدد المعيار ستة مبادئ للحوكمة الرشيدة لتقنية المعلومات والتي يمكن تطبيقها على معظم المؤسسات. هذه المبادئ تعبر عن السلوك المفضل لتوجيه عملية صنع القرارات المتعلقة بحوكمة تقنية المعلومات. بمعنى أن البيان الخاص بكل مبدأ يشير إلى ما يجب أن يتم تنفيذه، لكنه لم يحدد كيف أو متى أو بواسطة من سيتم تنفيذ هذه المبادئ، إذ إن هذه الجوانب تعتمد على طبيعة المنظمة التي ستقوم بتطبيق تلك المبادئ:

المبدأ الأول: المسؤولية: يتعين على الأفراد والجماعات داخل المؤسسة معرفة وقبول مسؤولياتهم فيما يخص كلاً من توفير وطلب خدمات وموارد تقنية المعلومات. فأصحاب المسؤوليات عن التدابير والإجراءات يملكون أيضاً سلطة تنفيذ تلك التدابير والإجراءات.

المبدأ الثاني: الإستراتيجية: إستراتيجية عمل المؤسسة يجب أن تأخذ بعين الاعتبار القدرات الحالية والمستقبلية لتقنية المعلومات؛ حيث ينبغي على هذه الخطط الإستراتيجية لتقنية المعلومات تلبية الاحتياجات الحالية والمستمرة الخاصة بإستراتيجية عمل المؤسسة.

المبدأ الثالث: الاقتناء: يجب أن تكون أسباب اقتناء عناصر وموارد تقنية المعلومات حقيقية ولها ما يبررها، وأن تكون قائمة على أساس عملية تحليلية مناسبة ومستمرة، وجاءت نتيجة قرارات واضحة وشفافة. ويجب أن يكون هناك توازن مناسب بين المنافع والفرص والتكاليف والمخاطر على المدى القصير والطويل.

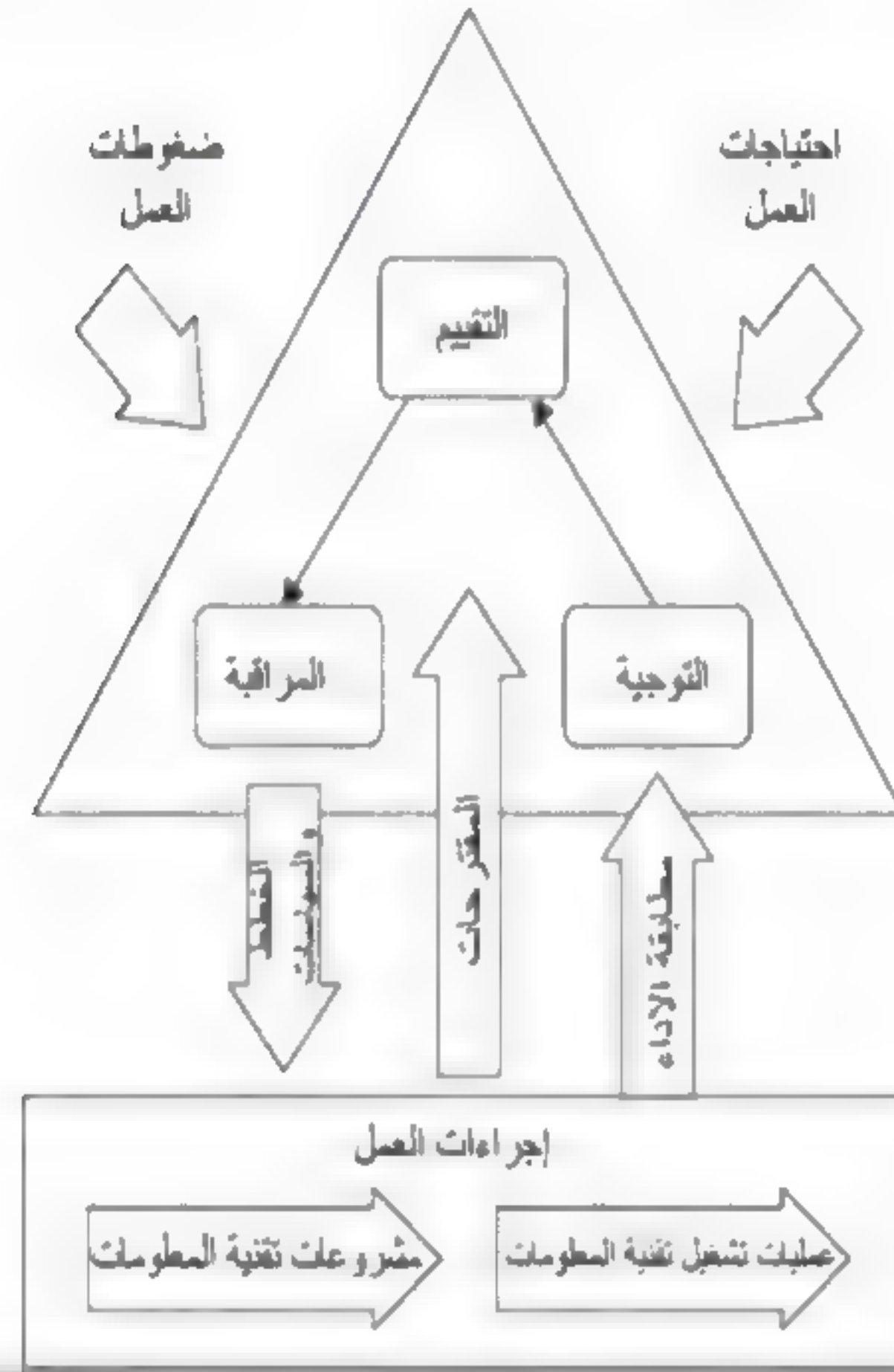
المبدأ الرابع: الأداء: يجب أن تكون تقنية المعلومات صالحة لأغراض دعم المؤسسة، وتقديم الخدمات، ومستويات الخدمة، وجودة الخدمات اللازمة لتلبية متطلبات المؤسسة الحالية والمستقبلية.

المبدأ الخامس: الأداء: يجب أن تكون تقنية المعلومات متوافقة مع جميع القوانين واللوائح التنظيمية الإلزامية ومع السياسات والإجراءات المحددة والمطبقة والمفروضة بشكل واضح.

المبدأ السادس: السلوك البشري: يجب على سياسات وإجراءات وقرارات تقنية المعلومات أن تُظهر احترامها للسلوك البشري، وأن تتضمن جميع الاحتياجات الحالية والمستحدثة للأشخاص المعنيين في العملية.

شكل توضيحي (٤-٧)

نموذج الأيزو ٣٨٥٠٠ لحوكمة تقنية المعلومات المؤسسية



بالإضافة إلى تلك المبادئ الأساسية، فإن المعيار يقدم أيضاً نموذجاً لحوكمة تقنية المعلومات. كما هو موضح في الشكل التوضيحي (٤-٧). فقد تم وصف العملية الشاملة لحوكمة تقنية المعلومات واحتياجات وضغوطات العمل التي تحتاج إلى بعض التغييرات والإجراءات في حوكمة تقنية المعلومات في مركز المثلث الموجود في الشكل التوضيحي (٤-٧). يوضح النموذج ضغوطات واحتياجات الأعمال التي تؤثر في العملية الخاصة بحوكمة تقنية

المعلومات. ثم تأتي بعد ذلك عمليات الحوكمة لتهيمن على مجمل عمليات تقنية المعلومات حيث تتأثر عمليات حوكمة تقنية المعلومات بالمقترحات المختلفة التي نشأت من تقنية المعلومات. كما تقوم عملية حوكمة تقنية المعلومات بتقديم الخطط والسياسات اللازمة لتقنية المعلومات، وتقوم إدارة تقنية المعلومات بأكملها بتقديم معلومات عن أداء وامثال حوكمة تقنية المعلومات. وقد تم وصف العملية الأساسية الشاملة في فصول أخرى من هذا الكتاب، إلا أن أن معيار أيزو ٣٨٥٠٠ يقوم بعمل جيد في احتواء هذه المسألة.

يوجد بداخل مثلث حوكمة تقنية المعلومات الموجود في الشكل التوضيحي (٧-٤)، ثلاث وظائف إجرائية هي التقييم والتوجيه والمراقبة. حيث يقدم معيار الأيزو تعريفاً محدداً لكل عملية من هذه العمليات على النحو التالي:

١. **التقييم:** يجب على كبار مديري تقنية المعلومات أن يقوموا بدراسة وإصدار القرارات المتعلقة بالاستخدام الحالي والمستقبلي لجميع موارد تقنية المعلومات. متضمناً ذلك الإستراتيجيات والمقترحات والترتيبات الخاصة بالإمدادات والتجهيزات (سواء كانت داخلية أم خارجية أو كليهما). أثناء تقييم استخدام تقنية المعلومات، ينبغي على الإدارة أن تأخذ في الحسبان الضغوط الخارجية أو الداخلية الناشئة عن الأعمال، مثل توجهات التغيير التقني أو التوجهات الاقتصادية أو التوجهات الاجتماعية، والتأثيرات السياسية.

ويجب أن تقوم الإدارة العليا بإجراء هذه التقييمات باستمرار كلما تغيرت ضغوطات الأعمال. ويجب عليها أيضاً أن تأخذ في اعتبارها كلاً من الاحتياجات الحالية والمستقبلية للأعمال - الأهداف التنظيمية الحالية والمستقبلية التي يجب تحقيقها، مثل الحفاظ على الميزة التنافسية. فضلاً عن أهداف محددة للإستراتيجيات والمقترحات التي يتم تقييمها.

٢. **التوجيه:** يجب على الإدارة العليا أن تقوم بتخصيص إدارة مسؤولية عن إعداد وتنفيذ الخطط والسياسات، ويجب أن تقوم بنفسها بالإشراف على هذه الإدارة. ويجب على هذه الخطط أن تحدد الاتجاه نحو الاستثمارات في مشاريع تقنية المعلومات وعملياتها التشغيلية. ويجب أن تضع هذه السياسات أسلوباً محدداً وواضحاً في استخدام تقنية المعلومات.

وينبغي أن يضمن المديرون أن عملية الانتقال من المشاريع إلى الحالة التشغيلية يتم التخطيط لها وإدارتها بشكل سليم، مع الأخذ بعين الاعتبار التأثيرات في ممارسات الأعمال والممارسات التشغيلية وكذلك النظم والبنية التحتية الحالية لتقنية المعلومات.

يجب أن تشجع الإدارة العليا لتقنية المعلومات على ثقافة الحوكمة الرشيدة لتقنية المعلومات عن طريق اشتراط المديرين توفير المعلومات في الوقت المناسب، لتتوافق مع التوجه وتتماشى مع المبادئ الستة للحوكمة الرشيدة.

٣. **المراقبة:** ينبغي على الإدارة العليا أن تراقب، من خلال استخدام نظم القياس المناسبة، الأداء العام لتقنية المعلومات. يجب أن يطمئنوا أنفسهم أن هذا الأداء يسير بحسب الخطط المعدة لذلك، وخاصة ما يتعلق بأهداف العمل. كما ينبغي على الإدارة أيضاً التأكد من أن تقنية المعلومات تتوافق مع الالتزامات التنظيمية والقانونية والتعاقدات الخارجية ومع ممارسات الأعمال الداخلية كذلك.

إرشادات لتطبيق معيار أيزو ٣٨٥٠٠:

قامت منظمة الأيزو بنشر هذا المعيار ووضع المبادئ الست الخاصة به في النموذج الخاص بحوكمة تقنية المعلومات لتقديم إرشادات أكثر تحديداً لحوكمة تقنية المعلومات. ويمكن شراء هذا الدليل الإرشادي وجميع التفاصيل المتعلقة بالمعيار أو تحميلها من الموقع الإلكتروني للأيزو (www.iso.org/iso/catalogue_detail?csnumber=51639). ولا تسمح لنا قوانين حقوق التأليف والنشر الخاصة بالأيزو بإعادة إنتاج هذه الإرشادات التي تم نشرها. ولكننا قمنا بتحرير واستخراج جزء صغير من هذه الإرشادات لتقديم بعض الرؤى عن قرب للمواد الفعلية.

إذا أخذنا مبدأ الإستراتيجية، مثلاً، فإن هناك إرشادات لكل خطوة من الخطوات اللازمة لإجراء التقييم والتوجيه والمراقبة. وعلى الرغم من التغيرات التي طرأت على المعيار الفعلي، وبالتأكيد لم نقصد أن نشرح المعيار الفعلي لأيزو ٣٨٥٠٠، فإن ما يلي يمثل إرشادات تتعلق بمبادئ من مبادئ المعيار:

• المبدأ الأول، إستراتيجية لتقييم ما يلي:

- ينبغي على الإدارة العليا تقييم التطورات الحاصلة في عمليات تقنية المعلومات والأعمال لديها لضمان أن تقنية المعلومات سوف تقدم الدعم الكافي للاحتياجات المستقبلية للأعمال.

- إذا أخذنا بعين الاعتبار الخطط والسياسات، فعلى الإدارة العليا تقييم أنشطة تقنية المعلومات لديها للتأكد من أنها تتماشى مع أهداف المؤسسة تبعاً للظروف المتغيرة، وتأخذ في الحسبان ممارسات أفضل، وتلبي المتطلبات الرئيسية الأخرى لأصحاب المصلحة.

• المبدأ الثاني، إستراتيجية لمراقبة ما يلي:

- يجب أن تقوم الإدارة العليا بمراقبة التقدم المحرز في المقترحات التي تمت الموافقة عليها لضمان أنها تحقق الأهداف في الأطر الزمنية المطلوبة باستخدام الموارد المخصصة.

- يجب أن تقوم الإدارة العليا بمراقبة استخدام تقنية المعلومات لضمان تحقيقها للفوائد المرجوة.

ويستمر المعيار باستخدام هذه اللغة العامة دون وجود أي قواعد محددة أو إجراءات تفصيلية، بل هناك فقط بعض الإرشادات العامة الجيدة. لكن عندما يدعو المعيار الإدارة العليا "لمراقبة التقدم المحرز في المقترحات التي تمت الموافقة عليها لضمان تحقيقها للأهداف ضمن الأطر الزمنية المطلوبة"، فإن هذا النوع من اللغة يشير إلى الحاجة إلى إجراءات للموافقة على مشروع وبرنامج تقنية المعلومات وتخطيط للمشروع مع وضع الأطر الزمنية، ومجرد مراجعات منتظمة من قبل الإدارة العليا. إن إدارة التدقيق الداخلي في المؤسسة. كما ذكرنا في الفصل التاسع عشر من هذا الكتاب، يمكن أن تكون بمثابة الخبير الاستشاري الداخلي الذي يساعد في تنفيذ هذه الإرشادات الخاصة بالمعيار، ويتحدث الفصل السادس عشر من هذا الكتاب، على سبيل المثال، عن أهمية إجراءات إدارة المشروعات.

هناك العديد من المعايير الأخرى لمنظمة الأيزو قابلة للتطبيق في هذا المجال، إلا أن المعيار أيزو ٣٨٥٠٠ يمكن أن يساعد ويقوي الحوكمة الشاملة لتقنية المعلومات المؤسسية.

وقد قام العديد من المديرين برفض بعض هذه المعايير لأنها كما يبدو تتطلب وثائق أو أعمالاً ورقية مكثفة أكثر من اللازم. بمعنى، إذا كان المعيار يقول: إن «على الإدارة أن تتابع» عملية أو نشاطاً ما، فإن جماعة المؤسسة التي تدعم هذا المجال يجب أن تكون في وضع يمكنها من إظهار نشاط المتابعة هذا من خلال مستوى معين من التوثيق. وبالتأكيد فإننا لا نقصد الحديث عن خزائن من العمل الورقي، ولكن نتحدث عن بعض أشكال الأدلة الإلكترونية القابلة للاسترجاع. لقد مرت العديد من مؤسسات اليوم والتي تقوم بتقديم منتجات أو خدمات في الأسواق العالمية من خلال عملية التدقيق الخارجي للأيزو للتصديق على امتثالها مع معايير الأيزو ٩٠٠٠. وقد نرى في السنوات القادمة متطلبات امتثال مشابهة لمعايير الأيزو الخاصة بحوكمة تقنية المعلومات عندما تصبح أكثر انتشاراً وقبولاً.

ملاحظات:

- ١- وليام إدواردز ديمينج (١٤ أكتوبر ١٩٠٠ - ٢٠ ديسمبر ١٩٩٣) كان أخصائياً، وأستاذاً ومؤلفاً، ومحاضراً وأستشارياً أمريكياً، وربما كان الأكثر شهرة بالنسبة لمجال عمله في اليابان، غير أنه كان زعيم حركة الجودة على مستوى العالم.

٢- Norman Ho, "ISO 9000: No Longer a Stranger to Service," Gartner, www.qualitydigest.com/june99/html/body_iso_9000.html

الفصل الثامن

قضايا حوكمة تقنية المعلومات: إرشادات حول إدارة المخاطر وإدارة المخاطر المؤسسية الصادرة عن لجنة المنظمات الراعية (COSO ERM) والمجموعة المفتوحة للامثال والأخلاقيات (OCEG)

تعد إدارة المخاطر أحد المفاهيم المرتبطة بالتأمين، فقد يتصور الفرد أو المؤسسة أن هناك نوعاً ما من التهديد، مثل خطر اندلاع حريق في أحد المباني السكنية أو سرقة، وعندها يقوم باتخاذ الإجراءات اللازمة لتوفير الحماية حال وقوع ذلك التهديد. إن الأسلوب الأكثر شيوعاً للحماية من المخاطر هو شراء تأمين من أحد الموردين الخارجيين التجاريين، أو تركيب آليات حماية للوقاية من المخاطر نوعاً ما. ويتم ذلك باستخدام نهج قائم على المخاطر لتحديد نوع التأمين ومقداره الذي يتم شراؤه أو نوعية الحماية اللازم توفيرها. وتعتمد العوامل الرئيسية لاتخاذ القرار هنا على حجم المخاطر أو التهديدات الأخرى المحتملة، كما تعتمد على تكاليف التأمين والأجهزة الوقائية اللازمة للحماية من تلك المخاطر.

وعلى الرغم من اعتقاد الناس في أغلب الأحيان بأن المخاطر والحماية الوقائية مرتبطة فقط بتهديدات كالحرائق أو الكوارث الطبيعية أو السرقة، فإن المؤسسة تكون في حاجة إلى أن تنظر إلى المخاطر من منظور أوسع من ذلك بكثير، وقد يشمل ذلك أموراً مثل الإخفاق في أحد المشاريع التجارية الجديدة أو الدعاوي الجنائية الناجمة عن عدم نجاح المنتج أو حدوث تحولات اقتصادية سلبية غير متوقعة. ولا تستطيع المؤسسة الحصول على تأمين - فعال وجيد من حيث التكلفة - بتلك السهولة لتغطية تلك المخاطر الأخرى فحسب، بل قد تحتاج إلى تنفيذ عمليات أخرى لتوفير الحماية من تلك المخاطر العديدة والمتنوعة الخاصة بالأعمال. وتكون موارد تقنية المعلومات المؤسسية غالباً أحد أكثر المجالات الرئيسية تعرضاً للمخاطر، حيث تمثل الخسارة المادية لمعدات تقنية المعلومات أو الاضطراب في شبكة الاتصالات أو سرقة مصادر البيانات أحد المخاطر الأساسية التي تهدد المؤسسة وقد يتبعها

عواقب وخيمة ما لم تكن هناك إدارة مناسبة للمخاطر وأدوات إصلاح قائمة ومعمول بها.

يناقش هذا الفصل أدوات إدارة المخاطر وتقنياتها من حيث أهميتها بالنسبة لحوكمة تقنية المعلومات، كما يقوم أيضاً باستعراض بعض أساسيات إدارة المخاطر التي يجب أن تمثل إحدى المجالات المعرفية المهمة لدى جميع مديري المؤسسات. ثم يقدم هذا الفصل بعد ذلك إطار إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية (COSO ERM)، وهو إطار متخصص في إدارة المخاطر المؤسسية صادر عن لجنة المنظمات الراعية (COSO) حيث يشبه إطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية (COSO) — الذي تم عرضه في الفصل الرابع من هذا الكتاب - إلا أن أهدافه مختلفة.

ويُختتم هذا الفصل بمقدمة عن نموذج الحوكمة وإدارة المخاطر والامتثال (GRC model) التابع للمجموعة المفتوحة للامتثال والأخلاقيات (OCEG)، مع التركيز على معايير إدارة المخاطر الخاصة بهذا النموذج. وتعمل المجموعة المفتوحة للامتثال والأخلاقيات (OCEG) وفق مجموعة من المعايير الصناعية التي قامت ببناء نموذج قدرة الحوكمة وإدارة المخاطر والامتثال (GRC capability model) الذي يركز بشكل قوي على إدارة المخاطر المؤسسية. وقد قامت هذه المجموعة (OCEG) بإطلاق مجموعة من المواد الخاصة بأفضل الممارسات في مجال الحوكمة وإدارة المخاطر والامتثال (GRC)، إلا أنها لم تكن بأهمية المعايير نفسها الخاصة بأحكام قانون ساربنز-أوكسلي (SOx instructions) أو معايير أيزو. وقد تم مناقشة كل منهما في فصول سابقة. ومع ذلك، فقد تحظى هذه المجموعة باعتراف وقبول عام في عالم الصناعة قريباً، وقد يكون الامتثال لمعايير تلك المجموعة أحد الأمور الهامة لحوكمة تقنية المعلومات.

أساسيات إدارة المخاطر:

سواء تم شراء وثيقة تأمين ضد الحريق لمرفق جديد بأحد المباني أم تم تثبيت أدوات وقائية لمشروع تجاري جديد أو شراء مستوى مناسب لما يعرف بالتأمين على مسؤوليات المديرين وكبار المسؤولين في المؤسسة، فعلى الإدارة العليا أن تدرك أنها تتعامل مع مجموعة

متنوعة من المخاطر المؤسسية التي يجب فهمها وإدارتها بشكل مناسب. ويجب التفكير في إدارة المخاطر على أنها عملية من أربع مراحل هي:

١. **تحديد المخاطر:** تحتاج المؤسسة إلى تحديد القضايا والظروف التي يمكن أن تصبح مخاطر مؤثرة في عمليات التشغيل الخاصة بها.

٢. **التقييمات الكمية أو النوعية للمخاطر الموثقة:** الخطوة التي تلي مرحلة تحديد المخاطر المحتملة، وهي توظيف الأدوات لتقدير الآثار المحتملة حال وقوع أي من هذه المخاطر المحددة.

٣. **تحديد أولويات المخاطر وتخطيط الاستجابة لها:** يجب أن تُعطى الأولوية للمخاطر الأكثر تأثيراً من بين المخاطر التي تم تحديدها، كما ينبغي وضع خطط استجابة لهذه المخاطر حال وقوعها.

٤. **متابعة المخاطر:** ينبغي وضع عمليات مستمرة لتقييم الأوضاع الحالية للمخاطر المحددة مسبقاً أو مخاطر جديدة واتخاذ الإجراء المناسب حال وقوع تلك المخاطر وتقييم التقدم المحرز في تلك الإجراءات العلاجية.

وينبغي أن تكون إدارة المخاطر عملية تتم على مستوى المؤسسة بأكملها، وتشمل جميع الأشخاص على المستويات كافة وفي جميع وحدات المؤسسة. وبينما تحتاج المؤسسات الكبيرة إلى تشكيل فريق متخصص في إدارة المخاطر، فإنه يجب على المؤسسات الصغيرة تعيين أشخاص ليكونوا مسئولين عن إدارة عملية تقييم المخاطر على مستوى مؤسستهم. فسواء تمت عملية إدارة المخاطر من خلال إدارة رسمية أم بجهود غير رسمية تخدم هذا الغرض، فإنه ينبغي أن تشمل إدارة المخاطر في المؤسسة طائفة عريضة من الناس من مستويات تنظيمية مختلفة في المؤسسة. فقد تكون وجهة نظر المدير المالي التنفيذي حول بعض مخاطر النظم المتعلقة بتقنية المعلومات مختلفة عن وجهة نظر المدير التنفيذي للمعلومات (CIO) أو أحد أعضاء الطاقم الخاص بعمليات تشغيل تقنية المعلومات. فكل منهم يرى المخاطر من وجهات نظر مختلفة. وينطبق هذا التشبيه ذاته على جميع جوانب المؤسسة.

ويجب تطبيق عملية إدارة المخاطر ذات المراحل الأربعة المذكورة سابقاً على جميع مستويات المؤسسة وبمشاركة مختلف الأشخاص. فسواء كانت المؤسسة صغيرة بها القليل من المرافق وتقع في منطقة جغرافية محدودة، أم كانت مؤسسة عالمية كبيرة، فإنه ينبغي تطوير أساليب عامة لإدارة المخاطر، وتعد هذه العملية مهمة وخصوصاً للشركات العالمية المنتشرة بكثرة هذه الأيام، وهي التي تحتوي على العديد من وحدات التشغيل المرتبطة بعمليات التشغيل والمرافق المختلفة الكائنة في مختلف البلدان. وقد تؤثر بعض مخاطر وحدة تشغيلية معينة في مخاطر وحدة تشغيلية أخرى أو تكون مرتبطة بها بشكل مباشر، غير أن الاعتبارات الخاصة بمخاطر أخرى قد تكون مستقلة بشكل فعال عن باقي المخاطر جميعاً. ويمكن أن تقع هذه المخاطر المشتركة بسبب توافر مجموعة مختلفة وكبيرة من الظروف تبدأ بقرارات مالية ضعيفة إلى تغيرات في مدى تجاوب المستهلكين مع اللوائح الحكومية الجديدة. وتعد العمليات الفعالة لإدارة المخاطر من العناصر المهمة لحوكمة فعالة لتقنية المعلومات.

تحديد المخاطر:

في الوقت الذي يتم فيه التركيز على حوكمة تقنية المعلومات والمخاطر المتعلقة بتقنية المعلومات، ينبغي مع ذلك تركيز الإدارة العليا على كل المخاطر التي قد تواجه المؤسسة، سواء تلك المتعلقة بتقنية المعلومات أم غيرها. كما ينبغي أن تسعى الإدارة إلى تحديد جميع المخاطر المحتملة التي قد تؤثر في نجاح المؤسسة، بدءاً من المخاطر الأكبر أو الأكثر تأثيراً بالنسبة لقطاع الأعمال بأكملها، وانتهاءً بالمخاطر الأقل أهمية وهي المرتبطة بالمشاريع الفردية أو بوحدات الأعمال الأصغر حجماً. كما تحتاج عملية تحديد المخاطر إلى اتباع نهج مدروس للنظر في المخاطر المحتملة في كل مجال من مجالات العمليات التشغيلية، ومن تحديد مجالات المخاطر الأكثر تأثيراً والتي يمكن أن تؤثر في كل عملية خلال فترة زمنية معقولة. ليس المقصود بالفكرة هنا مجرد سرد جميع المخاطر المحتملة، وإنما تحديد المخاطر التي قد تؤثر إلى حد ما في عمليات التشغيل خلال فترة زمنية معقولة. وقد تكون هذه ممارسة صعبة لأننا في كثير من الأحيان لا نفهم جيداً احتمالات وقوع المخاطر أو طبيعة عواقب مواجهة المؤسسة لتلك المخاطر.

يوجد لدى بعض المؤسسات وظيفة مدير تنفيذي للمخاطر يكون مسئولاً عن عمليات إدارة المخاطر في المؤسسة. ويتعين على الإدارة العليا حال غياب هذه الوظيفة أن تبني فريقاً خاصاً بإدارة المخاطر سواء كان ذلك بشكل رسمي أم غير رسمي، وذلك بهدف إدارة عمليات إدارة المخاطر، لديها. كما يجب أن يضم هذا الفريق جميع العناصر الهامة في المؤسسة ومن ضمنهم أعضاء من التدقيق الداخلي والإدارة القانونية والمكاتب الإدارية الرئيسية لقيادة الأنشطة الخاصة بإدارة المخاطر.

كما يجب إتمام عملية تحديد المخاطر التي يقوم بها فريق إدارة المخاطر على مستويات متعددة في المؤسسة. فالمخاطرة التي يكون لها تأثير في وحدة أعمال منفردة أو مشروع مستقل قد لا يكون لها تأثير كبير في المؤسسة بأكملها أو خارجها. وعلى العكس من ذلك، فإن إحدى المخاطر الرئيسية التي تؤثر في الاقتصاد بأكمله يمتد تأثيرها ليصل إلى المؤسسة الفردية ووحدات الأعمال المنفصلة التابعة لها. كما قد تكون بعض المخاطر الكبرى نادرة الحدوث، إلا أنها قد لا تزال كارثية بدرجة تجعل من الصعب تحديدها كحدث مستقبلي وارد الحدوث.

إن الطريقة الجيدة لبدء عملية تحديد المخاطر على مستوى المؤسسة هي وضع مخطط هيكلي تنظيمي رفيع المستوى للمؤسسة يسرد المستوى المؤسسي ووحدات التشغيل. وقد يكون لكل وحدة من هذه الوحدات مرافق في مواقع عالمية متعددة، كما قد تتكون أيضاً من عمليات تشغيل عديدة ومتنوعة. ويكون لكل مرفق منفصل بعد ذلك إداراته أو وحداته الخاصة به. وقد تكون بعض هذه المرافق المستقلة مرتبطة بعضها مع بعض بشكل وثيق، في حين يمثل البعض الآخر ما يتجاوز بقليل الاستثمارات التي تعكس التقارير المالية في المؤسسة. وقد يكون من الصعب والمعقد في بعض الأحيان إطلاق مبادرة على مستوى المؤسسة لتحديد جميع المخاطر في مختلف مجالاتها المستقلة. إن هذا النوع من الممارسات يمكن أن يحقق أحياناً نتائج مثيرة للاهتمام و/أو مثيرة للقلق. فعلى سبيل المثال، قد تكون الإدارة على مستوى الشركة على علم ببعض مخاطر المسؤولية القانونية عن المنتج، إلا أن مشرف الخطوط الأمامية في وحدة التشغيل قد ينظر إلى المخاطر نفسها من منظور مختلف تماماً.

كما ينظر أعضاء المؤسسة على مختلف المستويات إلى بعض هذه المخاطر ذاتها من وجهات نظر مختلفة. فمدير التسويق قد يشعر بالقلق إزاء إستراتيجيات التسعير الخاصة بالمنافس أو المخاطر الخاصة بأنشطة التسعير التي من شأنها أن تضع المؤسسة في موضع انتهاك للقوانين الخاصة بضبط التبادل التجاري. وقد يشعر مدير تقنية المعلومات بالقلق إزاء مخاطر فيروسات الحاسب أو هجومات البرمجيات الخبيثة على نظم التطبيقات؛ لكنه سيحتفظ بقليل من المعرفة عن تلك المخاطر الخاصة بمسألة التسعير. تكون الإدارة العليا عادة على علم بمستوى مختلف ومجموعة مختلفة من المخاطر أكثر من تلك الموجودة في أذهان فريق العمل المخصص للقيام بعمليات التشغيل. ومع ذلك، يجب على الأقل تحديد كل هذه المخاطر والنظر إليها على أساس وحدة تلو الأخرى وعلى مستوى المؤسسة بالكامل.

وحتى تكون عملية تحديد المخاطر فعالة، يتطلب الأمر أكثر بكثير من مجرد إرسال رسالة بريد إلكتروني إلى جميع مسئولي وحدات التشغيل مع طلب سرد المخاطر الرئيسية في الوحدات التشغيلية الخاصة بهم؛ فمثل هذا الطلب عادة ما ينتج عنه عدد كبير من الإجابات المتعارضة في ظل عدم وجود نهج مشترك. إن أفضل نهج في ذلك هو تحديد أشخاص من مختلف مستويات المؤسسة يُطالبون بأن يكونوا بمثابة مقيمين للمخاطر. لذلك ينبغي تحديد الأشخاص الرئيسيين من داخل كل وحدة من وحدات التشغيل والإدارة المالية وإدارة تقنية المعلومات وإدارة الأعمال. ويكون هدفهم جميعاً هو تحديد المخاطر في وحداتهم ثم المساعدة في تقديرها، تلك المخاطر التي تقع حول إطار نموذج تحديد المخاطر. ويمكن أن يقود هذا النوع من المبادرات مجموعة خاصة بإدارة المخاطر على مستوى المؤسسة، إن وجدت، أو يُضاف ضمن مهام إدارة تقييم الضوابط الداخلية مثل التدقيق الداخلي.

ولعل أحد الأساليب الفعالة هنا هو تحديد بعض مجالات مخاطر "المغالطة البهلوانية"^(*) Straw man العالية المستوى التي قد تؤثر في وحدات التشغيل المختلفة. ويمكن للأشخاص ذوي المعرفة بعد ذلك أن ينظروا في هذه المخاطر القائمة على الافتراض، كما يمكنهم أيضاً توسيعها بإضافة المزيد من المخاطر إليها أو التعديل عليها إذا اقتضى الأمر ذلك. ويوضح

(*) المغالطة البهلوانية أو رجل القش هي إحدى الادعاءات القائمة على تحريف الموقف المعارض، بتنفيذ شكل الحجة بحيث يوحي أن الحجة المعاكسة صحيحة. ويقصد بها هنا تحديد المخاطر المحتملة من وجهة نظر معينة ومن ثم استخدام ذلك كأساس تنطلق منه ورش عمل يتم عقدها بين المعنيين بهذا الأمر للعمل من "رجل القش" هذا نحو ما يعتقدون أنه المخاطر المحتملة (المترجم).

الشكل التوضيحي (٨-١) مثالاً لعينة من إطار عمل نموذج المخاطر المؤسسية، فهو يسرد بعض مجالات المخاطر الرئيسية التي قد تؤثر في المؤسسة، مثل المخاطر الإستراتيجية ومخاطر عمليات التشغيل والمخاطر المالية. وتعد تلك العينة أحد أنواع القوائم عالية المستوى التي قد يتعجل الرئيس التنفيذي بوضعها رداً على سؤال يطرحه أصحاب المصالح خلال الاجتماع السنوي مثل، "ما الذي يقلقك نهاية اليوم؟" لكنه بالتأكيد لا يسرد جميع المخاطر التي تتعرض لها المؤسسة، وإنما يعد هذا نوعاً من أنواع القوائم الأولية التي يمكن للمؤسسة استخدامها للبدء في عملية تحديد المخاطر تفصيلاً. ويمكن أن يجتمع المسؤولون في المؤسسة - وغالباً يكون الفريق المعين لإدارة المخاطر - مع الإدارة العليا ويقومون بطرح بعض الأسئلة من نوعية "ما يقلقك؟ ..." لتحديد تلك المخاطر العالية المستوى.

إن هذا النموذج العام الذي يتعلق بالمخاطر العالية المستوى على وجه الخصوص يمكن أن يعمل أساساً لتحديد مخاطر معينة تواجه مختلف وحدات المؤسسة على نحو أفضل. فعلى سبيل المثال، يقوم النموذج بإدراج "مخاطر استمرارية الأعمال" تحت "المخاطر التقنية". وينبغي أن يكون مدير تقنية المعلومات قادراً على توسيع هذه المخاطر لتكون في شكل قائمة طويلة من المخاطر التقنية التفصيلية المتعلقة باستمرارية الأعمال والتعافي من كوارثها. ويُعد مدير عمليات التشغيل هو مستخدم موارد تقنية المعلومات الذي قد ينظر إلى مخاطر استمرارية الأعمال من وجهة نظر مختلفة جداً ويعرض مخاطر أخرى جديدة مرتبطة بما قد يحدث إذا لم تُتاح خدمات تقنية المعلومات. ولفهم أفضل للمخاطر التي تواجه المؤسسة، فإنه يكون من الأفضل غالباً توسيع تلك القوائم لوضع مجموعة أكثر اكتمالاً للمخاطر المحتملة.

التقييم الكمي أو النوعي للمخاطر:

نشير هنا إلى خطوة هامة للغاية في عملية تقييم المخاطر وهي أخذ جميع المخاطر المحددة وترتيبها من حيث تأثيرها واحتمالية حدوثها. حيث تُوجد العديد من الطرق الرسمية التي يمكن استخدامها هنا وتكون غالباً معقدة رياضياً، ولأننا لا نقوم بتحليل محطة توليد كهرباء ممولة من الحكومة أو ما شابه ذلك، فإن المؤسسة تكون غالباً أفضل حالاً إذا ما استخدمت نهجاً بسيطاً ومباشراً لتقييم المخاطر بحيث يفهمه جميع أعضاء فريق الإدارة العليا المسئولة عن عملية إدارة المخاطر الخاصة بهم ويقبلونه.

شكل توضيحي (٨-١)
أنواع مخاطر الأعمال المؤسسية

المخاطر الإستراتيجية		
مخاطر العوامل الخارجية		مخاطر العوامل الداخلية
• مخاطر الصناعة		• مخاطر السمعة
• مخاطر الاقتصاد		• مخاطر التركيز الإستراتيجي
• مخاطر المنافس		• مخاطر دعم الشركة الأصل
• مخاطر التغييرات القانونية والتنظيمية		• مخاطر حماية براءات الاختراع / العلامات التجارية
• مخاطر احتياجات العملاء ورغباتهم		
مخاطر عمليات التشغيل		
مخاطر العملية	مخاطر الإمتثال	مخاطر الموظفين
• مخاطر سلسلة التوريد	• مخاطر بيئية	• مخاطر الموارد البشرية
• مخاطر رضا العميل	• مخاطر تنظيمية	• مخاطر تنقل العمالة
• مخاطر زمن الدورة	• مخاطر السياسات والإجراءات	• مخاطر حوافز الأداء
• مخاطر تنفيذ العملية	• مخاطر التقاضي	• مخاطر التدريب
المخاطر المالية		
مخاطر الخزينة	مخاطر ائتمانية	مخاطر تجارية
• مخاطر أسعار الفائدة	• مخاطر السعة	• مخاطر السلع الأساسية
• مخاطر صرف العملات الأجنبية	• مخاطر الضمان	• مخاطر فترة التنفيذ
• مخاطر توفر رأس المال	• مخاطر التركيز	• مخاطر القياس
	• مخاطر التعثر (التخلف عن السداد)	
	• مخاطر التسوية	

مخاطر البنية التحتية ونظم تقنية المعلومات		
مخاطر مالية	مخاطر تشغيلية	مخاطر تقنية
• مخاطر المعايير المحاسبية	• مخاطر التسعير	• مخاطر الوصول إلى المعلومات
• مخاطر إعداد الميزانية	• مخاطر قياس الأداء	• مخاطر استمرارية الأعمال
• مخاطر إعداد التقارير المالية	• مخاطر سلامة الموظف	• مخاطر الإتاحة
• مخاطر الضرائب		• مخاطر البنية التحتية
• مخاطر إعداد التقارير الرقابية		

وكما أوضحنا قبل قليل، فإنه يجب أولاً على المؤسسات ووحدات تشغيل الأعمال التابعة لها تحديد جميع المخاطر المؤثرة التي تواجه المؤسسة بكاملها. وينتج غالباً عن هذه الممارسة الخاصة بتجميع قائمة كهذه مجموعة كبيرة من المخاطر المحتملة يكون بعضها في كثير من الأحيان خارج نطاق فهم الإدارة العليا أو تقديرها. فمدير تقنية المعلومات، على سبيل المثال، قد يسلط الضوء على أحد المخاطر في إستراتيجية البنية الموجهة نحو خدمات تقنية المعلومات في المؤسسة، كما أوضحنا في الفصل الثالث عشر من هذا الكتاب، وهو الأمر الذي قد لا تفهمه أو تقدره السلطة التنفيذية للمؤسسة. وهنا يمكن لإدارة تقنية المعلومات أن تتقصى مدى تأثير هذه المخاطرة وسبب المطالبة بمزيد من الموارد للتصدي لها. وعلى أية حال، يجب أن تحتفظ الإدارة العليا بنهج توافقي تنظر من خلاله إلى مثل تلك المخاطر وكذلك إلى التكاليف المرتبطة بوضع الإجراءات التصحيحية لها. وبعد ذلك يجب عليهم موازنة هذه المخاطرة مع العديد من المخاطر الأخرى التي قد تم تحديدها.

وعلى الرغم من أن هناك العديد من الأساليب الرسمية المنشورة والخاصة بالعملية الرسمية لتحليل المخاطر، فإن المؤسسة تحتاج إلى نهج بسيط لكنه دقيق لتنظر من خلاله في جميع المخاطر التي تم تحديدها لتقرر أي منها يحتاج إلى إجراءات تصحيحية ومتابعة. ويمكن استخدام مجموعة متنوعة من الأساليب، تمتد من النهج الكيفي السريع نسبياً القائم على التخمين الأفضل وصولاً إلى بعض الأساليب الكمية التفصيلية والرياضية الخالصة. وتوضح الفكرة الكلية هنا في مساعدة الإدارة على اتخاذ قرار أفضل فيما يتعلق بأي من تسلسلات الأحداث المحتملة المحفوفة بالمخاطر التي قد تمثل القلق الأكبر لإدارة المؤسسة.

إن النهج البسيط الذي يكون فعالاً غالباً هو تبني قائمة المخاطر السابق مناقشتها وتعميمها على جميع المشاركين، ويتم في ذلك تحديد المخاطر أو غيرها من خلال استبيان يسأل عن كل مخاطرة من تلك المخاطر:

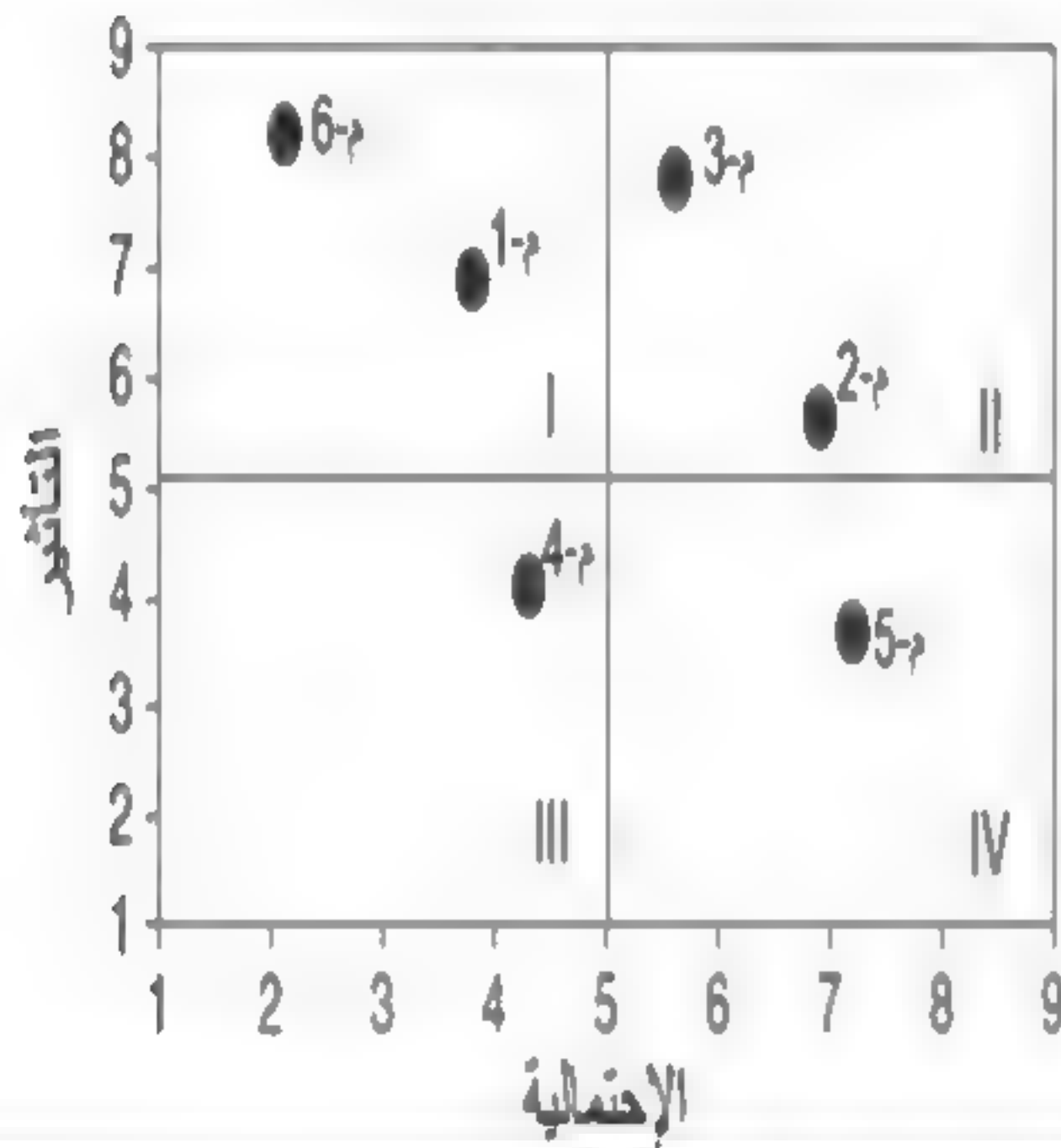
- ما مدى احتمالية حدوث مخاطرة ما خلال السنة القادمة تحديداً؟ مستخدماً الدرجات من ١-٩، قم بوضع درجة من رقم واحد لأفضل تخمين على النحو التالي:
- الدرجة ١ إذا كنت لا ترى تقريباً أي فرصة لحدوث هذه المخاطرة خلال تلك الفترة.
- الدرجة ٩ إذا كنت تشعر أن هذا الحدث سيحدث بشكل شبه مؤكد خلال تلك الفترة.
- الدرجات من ٢ إلى ٨ تعتمد على شعورك بأن الاحتمالية تقع بين هذين النطاقين.
- ما مدى تأثير المخاطرة من حيث التكلفة على المؤسسة؟ مرة أخرى باستخدام المقياس من ١-٩، ينبغي أن تعتمد نطاقات الدرجات على التأثير المالي للمخاطرة في المؤسسة. فالمخاطرة التي يمكن لتكاليفها أن تخفض أرباح المؤسسة حتى سنت واحد للسهم قد تكون مؤهلة للحصول على أقصى درجة، ٩.

ويجب توزيع الاستبيانات الخاصة بهذا النهج المبسط بشكل مستقل على الأشخاص ذوي المعرفة لتقييم كل مخاطرة من المخاطر التي تم تحديدها بالنسبة لهذين المقياسين (احتمالية الحدوث والتأثير) أو وضع درجة لها. ومثالاً على ذلك، لنفترض أن المؤسسة قامت بتحديد ستة مخاطر من م-١ إلى م-٦، وأنه يُطلب من أعضاء الفريق الخاص بتقييم المخاطر إجراء تقييم منفصل لكل مخاطرة من تلك المخاطر على حدة من حيث مقاييس احتمالية الحدوث والتأثير. بعد ذلك ومن خلال تطبيق هذين العاملين يُحسب متوسط هذه الدرجات، كما يتم رسمها على مخطط الرسم البياني، ذي الأجزاء الأربعة، الخاص بتحليل تقييم المخاطر كما هو مبين في الشكل التوضيحي (٨-٢). حيث يُظهر أن م-١ لها متوسط درجة احتمالية حدوث نحو ٣,٧٥ ودرجة تأثير ٧,٠٠، ويتم رسم هذه الدرجة في الربع الأول من المثال الخاص بمخطط تحليل تقييم المخاطر. ويدل هذا على أن م-١ تعتبر مخاطرة مؤثرة نسبياً لكن احتمالية حدوثها بعيدة جداً.

ويجب رسم جميع المخاطر التي يتم تحديدها بهذه الطريقة. فالمخاطر ذات احتمالية حدوث عالية وأكثر تأثيراً التي تنتهي في الربع الثاني، يجب أن تلقي المزيد من الاهتمام الفوري من قبل الإدارة.

شكل توضيحي (٢-٨)

مخطط تحليل تقييم المخاطر



وتعد النطاقات من ١ إلى ٩ هنا اعتبارية جداً؛ لذا ينبغي أن تحدد المؤسسة بعض الخطوط الإرشادية النسبية، لكن يجب على الموظفين فقط تقييم الأمور وفق رؤيتهم لاحتمالية الحدوث والتأثير النسبي للمخاطر التي تم تحديدها. كما يقدم هذا المخطط البياني الخاص بتحليل تقييم المخاطر مقياساً جيداً لفهم المخاطر المؤثرة المحيطة بالمؤسسة.

إن ما قامت به عملية تقييم المخاطر لا يتعدى وصف الأعمال التي تحتاجها المؤسسة عندما تقوم بتحديد عدد قليل نسبياً من المخاطر بشكل جيد. فمن السهل تماماً أن ننظر إلى الرسم البياني الخاص بتحليل تقييم المخاطر والتركيز على المخاطر العالية الاحتمالية

والتأثير في الربع الثاني - الأيمن العلوي - للتركيز على وضع خطط الإصلاح لتلك المخاطر. وعلى أية حال، فإنه في كثير من الأحيان، إذا كانت المؤسسة قد حددت مجموعة أكبر بكثير من المخاطر المحددة ومن النطاقات (من ١-٩) وكذلك المخططات في مثال الرسم البياني، فإن الرسم البياني لن يوفر تفاصيل كافية. ومن ثم فالنهج الأفضل هو التعبير عن هذه التقديرات المهمة والمؤثرة بدلالة عدد مكون من رقمين يمثل تقدير نسبة مئوية (على سبيل المثال، ٧٢٪) من تحقيق مخاطرة ما أو احتمالية (على سبيل المثال، ٧٢، ٠).

كما أن مجرد زيادة عدد الأرقام في النسبة مثلاً (٧، ٠) أو (٧٢، ٠) لن يزيد من دقة التقييم، لكنه يشير إلى أن فريق تقييم المخاطر يجب أن يكرس مزيداً من الاهتمام للحصول على تقديرات دقيقة. كما أن ذلك يساعد فرق التقييم في فهم العلاقة بين الاحتمالات التي تغطي الأحداث المستقلة وذات الصلة على نحو أفضل.

و على أية حال، تحتاج العملية الدقيقة لتقييم المخاطر إلى ما هو أكثر من مجرد تقديرات "التقديرات المرتفعة" سواء كانت ممثلة بنطاق مفرد (١-٩) أم نسبة مئوية كاملة من رقمين. كما يجب على فريق تقييم المخاطر وغيرهم من المهتمين أن ينظروا بحرص في المخاطر التي تُحدد أثناء عملية تحديد المخاطر، وينبغي جمع مزيد من المعلومات، إذا لزم الأمر. فعلى سبيل المثال، أثناء عملية تحديد المخاطر، قد يعتبر أحد المديرين أن الآثار المترتبة على القانون الجديد للتعرفة الجمركية يعد بمثابة مخاطرة مهمة، وربما يقوم آخرون في الجلسة نفسها بتوسيع التبعات بإضافة المزيد من المخاطر واعتبار أن القانون المفترض والمرتبب يعد بمثابة مخاطرة مؤثرة. وعلى أية حال، قبل وضع التصنيف القائم على الأهمية والتأثير، قد يرغب الفريق أو غيره من المديرين المسؤولين في القيام بمزيد من الأبحاث لتحديد التبعات الفعلية. ولربما في بعض الأحيان لا تكون هذه التبعات قابلة للتطبيق على الوحدة التشغيلية التي نحن بصدد الحديث عنها، أو أنه لن يكون لها أي تأثير يذكر حتى على مدار عدة سنوات قادمة. وتوضح النقطة الأساسية هنا في أن كل المخاطر التي تُحدد قد تحتاج إلى بعض المعلومات الإضافية لضمان تطبيقها بدقة.

تخطيط الاستجابة للمخاطر:

تَظهر قيمة متواضعةً حال نشر قوائم تفصيلية عن المخاطر المؤثرة ما لم تقم المؤسسة على الأقل باتخاذ بعض الخطوات الإجرائية الأولية إن (أو عندما) تتحمل المخاطرة. وتتضح الفكرة هنا في تقدير أثر تكلفة تحمل بعض المخاطر المحددة ومن ثم تطبيق تلك التكلفة على احتمالية عامل المخاطرة الخاص بالمخاطرة لاستنتاج القيمة المتوقعة للمخاطرة. كما يمثل هذا وقتاً مهماً لتحديد من هو المالك أو المسئول عن المخاطرة ومن هو الشخص أو الجهة المسئولة عن معرفة حالة المخاطرة المحددة ومتابعتها. ولا يحتاج هذا الإجراء في كثير من الأحيان إلى دراسات تفصيلية للتكاليف ولا إلى كثير من الاتجاهات والتقديرات التاريخية الداعمة. فقد تم تحديد المخاطر الخاصة بنا من خلال نهج العصف الذهني السريع الاستجابة دون تحليل تفصيلي، وبعد ذلك يقوم أشخاص ذوو معرفة بإجراء تقديرات احتمالية الحدوث والتأثير في ظل وجود المعرفة العامة عن المجال. كما يجب الانتهاء من حساب التكاليف المتوقعة، ويقوم بذلك العاملون في الخطوط الأمامية ويشملون أشخاصاً على مختلف مستويات المؤسسة يكون من المتوقع احتفاظهم ببعض المعرفة.

وتتضح الفكرة هنا من خلال المرور على كل مخاطرة تم تحديدها — وإذا كان الوقت محدوداً، فإنه يكفي فقط المرور على المخاطر الرئيسية — وتقدير تكاليف تحمل المخاطر المحددة. ويوضح الشكل التوضيحي (٨-٢) ست عينات لمخاطر تم رسمها باستخدام التقديرات الخاصة باحتمالية الحدوث والتأثير لكل مخاطرة. وهنا تمثل النواتج المشتركة لحاصل ضرب التأثير والاحتمالية درجة من درجات تقييم المخاطرة، وبترتيب هذه الدرجات تصبح القيمة الأعلى هي عنصر المخاطرة الأكبر الذي يدعو للقلق والاهتمام.

ويجب على فريق تقييم المخاطر النظر في أثر تكلفة كل مخاطرة من المخاطر المحددة وتقدير التكلفة الإجمالية على المؤسسة حال وقوعها. كما يوجد العديد من الطرق لوضع مثل هذه التقديرات الخاصة بتكلفة المخاطر، إلا أنه يجب استخدام النهج نفسه مع جميع المخاطر التي تم تحديدها. وبناءً على ذلك، يصبح حاصل ضرب درجة المخاطرة وتأثير التكلفة هو التكلفة أو الخسارة المتوقعة التي ستتكبدها المؤسسة حال وقوع المخاطرة

المحددة. ويوضح الرسم البياني في المثال أنه على الرغم من أن المخاطرة م-5 بها أعلى احتمالية حدوث، فإن تأثير التكلفة الأعلى للمخاطرة م-2 قد يسبب قلقاً إدارياً أكبر بكثير من المخاطرة م-5.

من المؤكد عدم دقة عينة تحليل المخاطر هذه، إلا أنها توضح أحد أنواع التفكير الذي نحتاج إليه لتقدير تكاليف التعافي من بعض وقائع المخاطر. في كثير من الأحيان يكون من السهل التعرف على بعض وقائع المخاطر، لكن الأكثر صعوبة في الغالب هو تحديد تكلفة التعافي من تلك المخاطرة. وعلى النحو المقترح طوال هذا الفصل، لا توجد حاجة لإجراء تحليلات تفصيلية تستغرق الكثير من الوقت، بل يكفي الاستعانة بأهل العلم الذين يفهمون مجال المخاطرة لإعطاء بعض التقديرات. كما يتعين على الفرق في الكيانات التي قد تتحمل هذه المخاطر المحددة أن تقدر التكاليف على أسس هي:

- تقدير التكلفة لأفضل الحالات التي يكون من الضروري فيها تحمل المخاطرة. يظهر هذا الافتراض فقط في حال وجود تأثير محدود عند حدوث المخاطرة.
- تقدير تكلفة العينة التي يقوم بها الشخص صاحب المعرفة.
- القيمة أو التكلفة المتوقعة لتحمل المخاطرة. هذا هو نوع المخاطرة الذي قد يشمل تكاليف أساسية وغير ذلك من العوامل مثل العمل الإضافي.
- تقدير التكلفة لأسوأ الحالات التي يكون من الضروري فيها تحمل المخاطرة. ويعد هذا أحد أنواع التقدير "إذا كان كل شيء يسير على نحو خاطئ".

لقد اقترحنا استخدام هذه التقديرات نقطة بداية لتشكيل فكرة عن حدود التكاليف التي تدور في خلد مختلف الأفراد، ومع ذلك فإننا نؤكد أن هذا مجرد نهج عالي المستوى. ويجب أن تعمل الإدارة العليا مع فرق الدعم المسئولة عن تقييم المخاطر لديها لفهم العمليات المعمول بها في المؤسسة.

ويعد الشكل التوضيحي (٨-٣) مثلاً على تخطيط ترتيب المخاطر. فخلية "القيمة المتوقعة" ليست سوى حاصل ضرب خلايا "أثر التكلفة" و"درجة المخاطرة". ويُقدّر هذا الرقم التكلفة التي ستتكبدها المؤسسة حال تحملها مخاطرة ما. وعلى الرغم من أن

الأرقام التي اختيرت لهذه العينات أرقام اعتباطية، فإنها توضح للمديرين أو أخصائيي إدارة المخاطر المؤسسية (ERM) كيفية تفسير هذه النوعية من التحاليل والعمل بمقتضاها.

فالمخاطرة م-٣، على سبيل المثال، بها احتمالية عالية وتأثير عالٍ، وكذلك التكلفة المتوقعة للتصحيح تكون عالية نسبياً. كما أن هذا النوع من المخاطر هو الذي ينبغي أن تحدده الإدارة على أنها أحد المخاطر المرشحة لاتخاذ إجراءات تصحيحية حيالها. ومع ذلك، فإن المخاطرة التالية في الجدول، المخاطرة م-٢، تنتمي أيضاً إلى الجانب الأيمن العلوي من الشكل الرباعي لكن بتكلفة عالية نسبياً لمعالجتها. وقد يكون هذا أحد نوعيات المخاطر التي بناءً عليها ستقرر الإدارة إذا ما كانت ستقبل المخاطرة أو تطور شكلاً آخر من خطة العلاج كما سيتم مناقشته لاحقاً.

شكل توضيحي (٣-٨)

مثال تخطيط الاستجابة طبقاً لتقييم المخاطر

المخاطرة	التأثير	الاحتمالية	درجة المخاطرة	التقييم	أثر التكلفة	قيمة الخسارة المتوقعة للمخاطرة
م-٣	٨,٠	٥,٧	٤٥,٦	١	١٢٠,٦٠٠ \$	٥,٤٩٩,٣٦٠ \$
م-٢	٥,٥	٧,٠	٣٨,٥	٢	٧٨٥,٠٠٠ \$	٣٠,٢٢٢,٥٠٠ \$
م-٥	٣,٩	٧,٢	٢٨,١	٣	١٥,٠٠٠ \$	٤٢١,٢٠٠ \$
م-١	٦,٨	٣,٨	٢٥,٨	٤	٢٧,٢٥٠ \$	٧٠٤,١٤٠ \$
م-٤	٤,٢	٤,٣	١٨,١	٥	٥٢,٣٥٠ \$	٩٤٥,٤٤١ \$
م-٦	٨,٤	٢,٠	١٦,٨	٦	١,٢٠٠ \$	٢٠,١٦٠ \$

ونؤكد مرة أخرى ارتفاع تكلفة المخاطرة، وفي هذه الحالة يكون تأثيرها مرتفعاً نوعاً ما، لكن احتمالية حدوثها تكون منخفضة للغاية. وهذه هي نوعية الأرقام التي تقرر الإدارة غالباً من خلالها أن "تأمل خيراً" وتعيش مع المخاطرة. وبالنسبة لمثل تلك المخاطرة، فإنها ستكلف الإدارة إذا ما قررت تحملها، كما ستكون مُكَلَّفَةً حال تثبيت بعض الأدوات الخاصة بالإجراءات التصحيحية. وعلى افتراض أن فريق إدارة المخاطر المؤسسية قام بعمل جيد في

إعداد تقديرات المخاطر تلك التي تم تحديدها، فهذا يمكن أن يكون نهجاً مفيداً في اتخاذ القرارات المتعلقة بالمعالجة المستمرة للمخاطرة.

متابعة المخاطر:

بينما يلزم عمل مسح للمخاطر المحتملة في البيئة المؤسسية ثم تقدير تكاليف واحتمالات تلك المخاطر التي قد تحدث، فإنه يلزم القيام بهذا الإجراء لأكثر من مرة. بل يجب وضع عمليات رسمية لمتابعة المخاطر وفحص حالتها، فضلاً عن معرفة المخاطر الجديدة المحتملة بشكل مستمر. إن متابعة المخاطر هي عملية توصيف الوضع الحالي للمخاطر المحددة وتحليله وكذلك تتبع المخاطر الجديدة المحتملة حال ظهورها. فهي تضمن أن موارد الشركة المخصصة للمشروع تعمل بشكل صحيح.

إن هذا المفهوم الخاص بتثبيت أدوات متابعة سيظهر في كثير من العمليات الأخرى الخاصة بحوكمة تقنية المعلومات التي تمت مناقشتها في فصول لاحقة. فعلى سبيل المثال، يناقش الفصل الرابع عشر من هذا الكتاب إدارة حوكمة تقنية المعلومات وإدارة محفظة استثمارات تقنية المعلومات، في حين يقدم الفصل السادس عشر من هذا الكتاب للقارئ، ما يعرف بالإدارة الفعالة لمحفظة المشاريع والبرامج. وفي تلك الحالات وغيرها، تحتاج المؤسسة إلى وضع ضوابط رقابية لتقييم الحالة بشكل مستمر.

وفي الماضي لم تكن العديد من أدوات المتابعة هذه موجودةً بشكل واقعي في العديد من مجالات النظم التقليدية مثل تقنية المعلومات. فقد كان طاقم تقنية المعلومات في كثير من الأحيان يترقبون بكل أمل أن تسير الأمور بسلام وألا تتعطل النظم الرئيسية. وإذا ما حدث ذلك وتعطلت تلك النظم وما يصاحبها من تداعيات، تظهر عادةً حالةً من الزخم تهدف إلى استعادة تلك النظم للعمل مرة أخرى. وفي السنوات الأخيرة فقط تم وضع العديد من أفضل تطبيقات تقنية المعلومات التي تم استخدامها وتطبيقها مع أدوات متابعة لتسليط الضوء على حالات المشاكل.

كان لدينا تجربة أفضل بكثير مع أدوات المتابعة في بيئة إدارة المخاطر، إذ كلُّ من إنذار الحريق التقليدي المثبت على الحائط أو جهاز الإنذار المستخدم في الكشف عن السرقات

المثبت على الباب يعتبر من النظم التقليدية لمتابعة المخاطر. ومن خلال استخدام التقارير الشبيهة بلوحة معلومات الإدارة أو غيرها من الآليات، يجب على المؤسسة أن تضع نظم متابعة للتحقق من الوضع الحالي للمخاطر الرئيسية المحددة وكذلك أجهزة إنذار الإشارة عند الحاجة إلى اتخاذ إجراءات تصحيحية. وعلى الرغم من عدم قيام أحد كبار المديرين ببناء أدوات المتابعة هذه أو تصميمها بوجه عام، فإن هذا المسئول التنفيذي نفسه ينبغي أن يكون في موقع يؤهله لطرح الأسئلة حول وضع أدوات متابعة مخاطر المؤسسة.

تعريفات إدارة المخاطر المؤسسية وأهدافها الصادرة عن لجنة المنظمات الراعية (COSO ERM): عرض محفظة المخاطر:

تحدثنا في الفصل الرابع من هذا الكتاب عن إطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية (COSO) وأهميته على أنه أداة لتقييم الضوابط الداخلية للمؤسسة وتعزيز حوكمة تقنية المعلومات. ويعد إطار إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية (COSO ERM) أداة مماثلة لهذا الإطار غير أنه يختلف عنه، فإطار المخاطر المؤسسية هذا من شأنه أن يساعد المؤسسات على أن تحتفظ بتعريف ثابت عن المقصود بالمخاطر على مستوى المؤسسة التي ينبغي أن تؤخذ بعين الاعتبار وبشكل متناسق عبر المؤسسة بأكملها. لقد قامت لجنة المنظمات الراعية (COSO) بإطلاق إطار إدارة المخاطر المؤسسية بطريقة مشابهة لإطار الرقابة الداخلية الخاصة بها والذي تم تطويره في وقت سابق. كما تم تشكيل مجلس استشاري يتكون من أعضاء من المؤسسات الراعية وتم التعاقد مع شركة برايس ووترهاوس كوبرز (Pricewaterhouse Coopers (PWC على تطوير وصف الإطار وصياغته. وقد تم نشر الوصف الخاص بالإطار عام ٢٠٠٤، والصفحات التالية من هذا الفصل تلخص مفاهيم إطار إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية. وعلى أية حال، فإننا ندعو القارئ أيضاً إلى الوصول إلى وصف كامل لإطار إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية. إذ يمكن تحميل نسخة كاملة من إطار إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية أو شراؤها، وكذلك بعض المواد المختصرة الداعمة من خلال معهد المحاسبين القانونيين الأمريكيين (AICPA) أو موقع الويب الخاص بلجنة المنظمات الراعية من خلال الرابط التالي: www.coso.org

وكما بدأ إطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية باقتراح تعريف ثابت للموضوع الذي يتناوله، يبدأ إطار إدارة المخاطر المؤسسية أيضاً من خلال تعريف إدارة المخاطر المؤسسية على النحو التالي:

إن إدارة المخاطر المؤسسية هي عملية يقوم بها مجلس إدارة الكيان والإدارة وغيرهم من الموظفين، ويكون تطبيقها في شكل إستراتيجية يتم وضعها في جميع أرجاء المؤسسة، وتكون مصممة لتحديد الأحداث المحتملة التي قد تؤثر في الكيان، وكذلك تدير المخاطر لتكون في نطاق قدرة الكيان على تقبل المخاطر، وتقدم ضماناً معقولاً بتحقيق أهداف الكيان.

وحيث إن هذا هو تقريباً التعريف الأكاديمي، فإنه ربما يتعين على المرء النظر في النقاط الرئيسية لإدارة المخاطر المؤسسية الصادرة عن لجنة المنظمات الراعية وتذكرها، والتي من ضمنها:

- إدارة المخاطر المؤسسية عبارة عن عملية. رغم أن تعبير "عملية" يُساء استخدامه غالباً، فإن القاموس يعرفها على أنها مجموعة من الإجراءات الرامية إلى تحقيق نتيجة. وفضلاً عن أن هذا التعريف لا يخدم العديد من المهنيين، فإن الفكرة هنا هي إدراك أن العملية ليست إجراءً ثابتاً مثل استخدام شارة الموظف التي ما صُممت ولا طبقت إلا للسماح فقط لأشخاص معينين لدخول أحد المرافق المؤمنة. فمثل هذا الإجراء الخاص بالشارة - الذي يعتبر بمثابة مفتاح القفل - ما هو إلا مجرد إجراء خاص بالسماح أو عدم السماح بدخول شخص ما إلى أحد المرافق. وتميل العملية إلى أن تكون ترتيباً أكثر مرونة. ففي عملية اعتماد الإقراض مثلاً، يتم وضع قواعد قبول مع وجود خيارات لتعديلها عند حدوث اعتبارات أخرى. فالمؤسسة هنا قد تلوي قواعد الإقراض من أجل عميل غير مستحق للاقتراض يعاني من مشكلة على المدى القصير. فعملية إدارة المخاطر المؤسسية هي هذا النوع من العمليات. ولا تستطيع المؤسسة في كثير من الأحيان تحديد قواعد إدارة المخاطر من خلال كتاب قواعد صغير ومنظم بشكل محكم. بل، ينبغي أن تكون هناك سلسلة من الخطوات الموثقة لمراجعة وتقييم المخاطر المحتملة واتخاذ الإجراءات المناسبة استناداً إلى مجموعة واسعة من العوامل الموجودة في جميع أرجاء المؤسسة.

- يقوم أفراد يعملون في المؤسسة بتنفيذ عملية إدارة المخاطر المؤسسية. لن تكون إدارة المخاطر المؤسسية فعالة إذا تم تنفيذها فقط من خلال مجموعة من القواعد التي يتم إرسالها لوحدة التشغيل من المركز الرئيسي للشركة، البعيد عن تلك الوحدات التشغيلية، حيث يوجد هؤلاء الأشخاص العاملون بالشركة ممن قاموا بصياغة مسودة القواعد، وقد يكون لديهم القليل من فهم العوامل المختلفة المحيطة بهم التي يتم اتخاذ القرار بناءً عليها. ويجب أن يقوم على إدارة المخاطر أفراداً على مقربة كافية من مكان تلك المخاطر وحالها لفهم مختلف العوامل المحيطة بتلك المخاطر متضمناً ذلك آثارها.
- يتم تطبيق إدارة المخاطر المؤسسية من خلال وضع إستراتيجيات عبر المؤسسة بالكامل. تتعرض المؤسسات دائماً إلى إستراتيجيات بديلة متعلقة بمجموعة ضخمة من الإجراءات المستقبلية المحتملة. فمثلاً، هل يتوجب على الكيان أن يقتني أعمالاً تكميلية أخرى أم يكتفي فقط ببنائها داخلياً؟ وهل ينبغي تبني تقنية جديدة في عمليات التصنيع أم الاكتفاء بالتمسك بالأسلوب المجرب والصحيح؟ إن الإدارة الفعالة للمخاطر المؤسسية يجب أن تلعب دوراً رئيسياً في وضع تلك الإستراتيجيات البديلة. وبما أن هناك العديد من المؤسسات الكبيرة التي تحتوي على العديد من وحدات التشغيل المختلفة، فإنه ينبغي تطبيق إدارة المخاطر المؤسسية عبر تلك المؤسسة بأكملها باستخدام نوع من أنواع أساليب المحافظ الذي يقوم بدمج أنشطة المخاطر العالية والمنخفضة بعضها مع بعض.
- يجب الأخذ في الاعتبار مفهوم الرغبة في المخاطر. الرغبة في المخاطرة هي مقدار المخاطرة، على المستوى العام، الذي تكون المؤسسة ومديروها على استعداد لقبوله في سعيها لتحقيق القيمة المطلوبة. ويمكن قياس الرغبة في المخاطر من خلال الحس النوعي الذي يقوم على تصنيف المخاطر إلى فئات مثل عالية أو متوسط أو منخفضة؛ وبدلاً عن ذلك، يمكن تعريفها بطريقة نوعية. إن فهم الرغبة في المخاطر يغطي مجموعة واسعة من القضايا التي سيتم مناقشتها بمزيد من التفاصيل في الفصل العاشر من هذا الكتاب حول مخاطر الحوكمة ومخاطر أمن تقنية المعلومات التي تمت الإشارة إليها في فصول لاحقة تدور حول تطبيق حوكمة تقنية المعلومات. إن الفكرة الأساسية هنا هي أنه يجب أن يكون لدى كل مدير وكل مؤسسة عموماً مستوى ما من الرغبة في المخاطر.

فالبعض سيقبل بالمشاريع المحفوفة بالمخاطر التي تبشر بتحقيق عوائد عالية، في حين يفضل البعض الآخر أكثر المشاريع المنخفضة المخاطر المضمونة العائد. كما يستطيع المرء أن يتصور هذا المفهوم الخاص بالرغبة في المخاطرة أو أن يقيسه على اثنين من المستثمرين الافتراضيين. فأحدهما قد يفضل سوق المال أو الصناديق ذات المؤشرات المنخفضة المخاطر جداً إلا أن عوائدها تكون عادة منخفضة، في حين قد يستثمر الآخر في أسهم شركات التقنية الصغيرة الناشئة.

• **توفر إدارة المخاطر المؤسسية ضماناً معقولاً فقط وليس إيجابياً حول إنجازات الأهداف.** والفكرة هنا تتضح في أن إدارة المخاطر المؤسسية، مهما كانت مدروسة أو مُنفذة بشكل جيد، لا يمكن أن تمد الإدارة أو غيرها بأي ضمان مؤكد للنتائج. إن المؤسسة الخاضعة للرقابة بشكل جيد من خلال أشخاص على جميع المستويات تعمل باستمرار نحو تبني أهداف مفهومة وقابلة للتحقيق. وقد تتحقق تلك الأهداف فترة بعد فترة، حتى إن كان ذلك على مدى عدة سنوات. ومع ذلك، من الممكن أن يقع خطأ بشري غير مقصود أو سلوك غير متوقع من قبل آخرين، أو حتى وقوع كارثة طبيعية. فتسونامي^(١) (موجات المد البحري العاتية) التي حدثت في المحيط الهندي في ديسمبر عام ٢٠٠٤ يعد مثلاً على تلك الأحداث غير المتوقعة. إذ سُجل أن آخر موجة تسونامي في هذا الجزء من العالم قد حدثت منذ نحو ٤٠٠ عام مضت. وعلى الرغم من تطبيق عملية إدارة مخاطر مؤسسية فعالة، فإن المؤسسة قد تتعرض لمثل هذا الإخفاق غير المتوقع بالمرّة نتيجة لتلك الأحداث غير المتوقعة، فالتأكيدات المعقولة لا توفر ضماناً مطلقاً.

• **تم تصميم إدارة المخاطر المؤسسية للمساعدة في تحقيق إنجاز الأهداف.** يجب أن تعمل المؤسسة، من خلال إدارتها، على وضع أهداف مشتركة عالية المستوى يمكن أن يتشارك فيها جميع أصحاب المصلحة. ومن أمثلة ذلك، كما وردت في وثائق إطار (COSO ERM)، أمورٌ مثل تحقيق السمعة الإيجابية والحفاظ عليها داخل مجتمعات الأعمال والمجتمعات الاستهلاكية للمؤسسة وتقديم تقارير مالية موثوقة لجميع أصحاب المصلحة والتزام المؤسسة بالقوانين واللوائح. إن البرنامج العام لإدارة المخاطر المؤسسية من شأنه أن يساعد المؤسسة على تحقيق تلك الأهداف.

وتكون الأهداف والغايات المتعلقة بإدارة المخاطر المؤسسية قليلة القيمة ما لم تكن منظمة ومتناغمة معاً بطريقة تمكن الإدارة من أن تنظر في الجوانب المختلفة لهذه المهمة وأن تفهم - نوعاً ما على الأقل - الطريقة التي تتفاعل بها بعضها مع بعض على نحو متعدد الأبعاد. هذه هي القوة الحقيقية لنموذج إطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية (COSO)؛ فهو يصف على سبيل المثال، كيف أن التزام المؤسسة بالقوانين واللوائح يمكن أن يؤثر في جميع مستويات الضوابط الداخلية، من عمليات المتابعة إلى بيئة الرقابة، وكيف أن هذا التوافق مهم لجميع كيانات المؤسسة أو وحداتها. وبطريقة مماثلة، قامت لجنة المنظمات الراعية (COSO) بتطوير نموذج إطار إدارة المخاطر المؤسسية الذي يوفر بعض التعريفات الشائعة لإدارة المخاطر، والمساعدة على تحقيق الأهداف الرئيسية للمخاطر في جميع أنحاء المؤسسة.

إطار إدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية (COSO ERM):

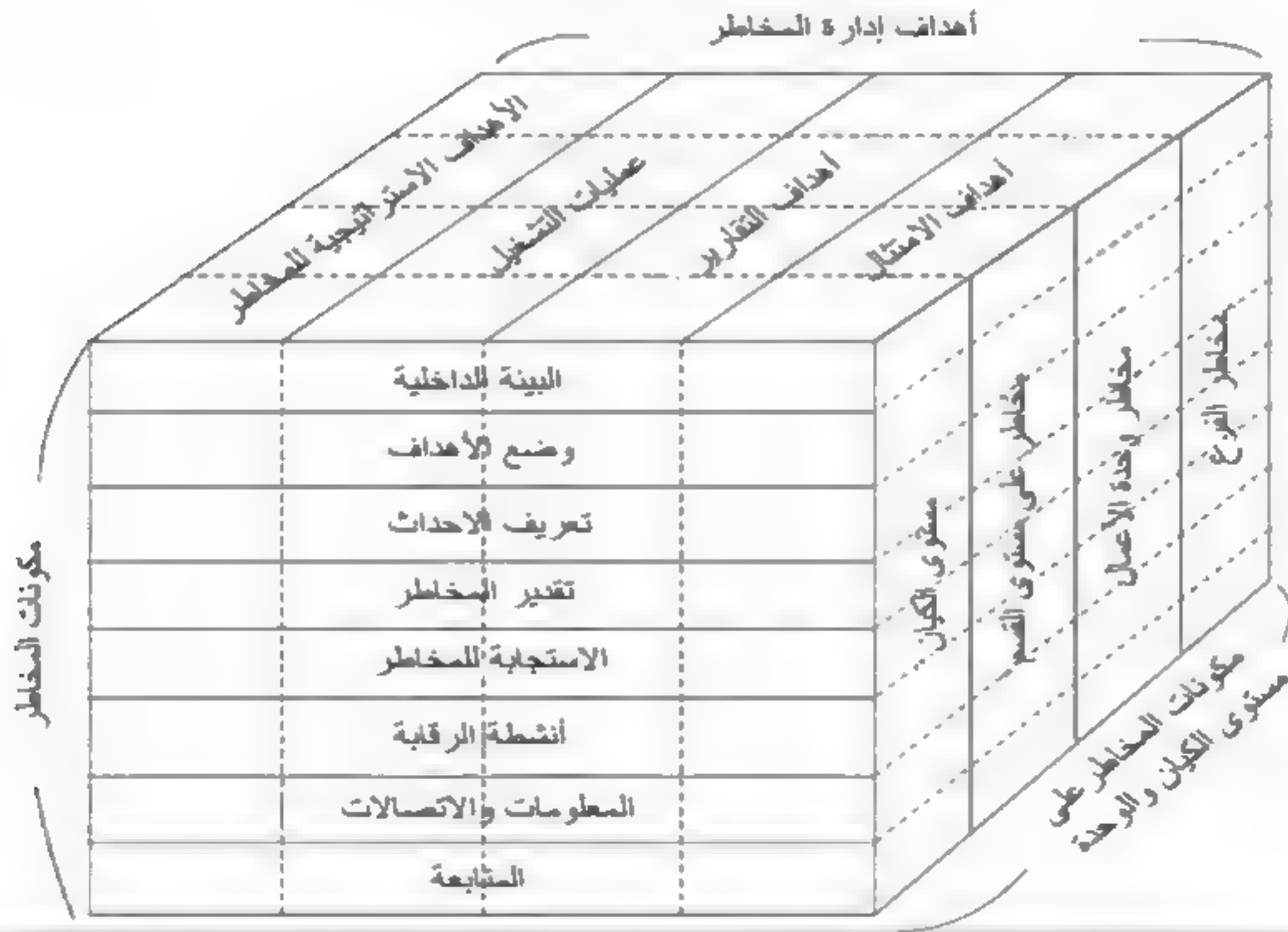
إن إطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية (COSO)، كما نوقش في الفصل الرابع من هذا الكتاب، وتم وصفه في الشكل التوضيحي (٤-١)؛ أصبح نموذجاً يحتذى به في جميع أنحاء العالم، فهو يقوم بعمل فعال جداً في وصف الضوابط الداخلية وتحديثها. وقد يبدو إطار (COSO ERM) من الوهلة الأولى مشابهاً جداً لإطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية (COSO) ربما لأن بعض أعضاء الفريق نفسه قد تم ضمهم إلى كل من مشروع الرقابة الداخلية ومشروع إدارة المخاطر المؤسسية. إن إطار (COSO ERM) كما هو موضح في الشكل التوضيحي (٤-٨) عبارة عن مكعب ثلاثي الأبعاد يحتوي على المكونات التالية:

- أربعة أعمدة رأسية تمثل الأهداف الإستراتيجية للمخاطر المؤسسية.
- ثمانية صفوف أفقية وهي مكونات المخاطر.
- عدة مستويات للمؤسسة، بدءاً من مستوى كيان "المقر الرئيسي" إلى مستوى الفروع الفردية. وتبعاً لنوع المؤسسة، قد توجد هنا "شرائح" كثيرة للنموذج.

يقوم هذا القسم بتسليط الضوء على بعض المكونات الأفقية لإطار (COSO ERM). كما يمكن الحصول على وصف أكثر تفصيلاً لإدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية (COSO ERM) ومكوناته الثلاثية الأبعاد، وكيفية ارتباطها معاً من خلال زيارة الموقع www.coso.org ومن خلال الوصف الأكثر تفصيلاً لإدارة المخاطر المؤسسية الصادر عن لجنة المنظمات الراعية (COSO ERM) المقدم من مؤلف هذا الكتاب^(٣). كما يوفر إطار إدارة المخاطر المؤسسية (ERM) نموذجاً للمؤسسات لدراسة الأنشطة ذات الصلة بالمخاطر وفهمها على جميع مستويات المؤسسة بالإضافة إلى كيفية تأثير هذه الأنشطة بعضها على بعض. وكجزء من فهم حوكمة تقنية المعلومات يهدف هذا الكتاب إلى مساعدة كبار المديرين على فهم المخاطر التي تواجه مؤسساتهم وإدارتها على نحو أفضل.

شكل توضيحي (٨-٤)

إطار COSO لإدارة المخاطر المؤسسية



يبدو أن هذا الوصف الخاص بإطار (COSO ERM) يشبه إلى حد بعيد إطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية (COSO) الذي أصبح مألوفاً لدى العديد من

المهنيين. فعندما تم إطلاق إطار (COSO ERM) لأول مرة اعتقد البعض للوهلة الأولى اعتقاداً خاطئاً بأنه مجرد تحديث لإطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية (COSO) الأكثر شيوعاً لديهم. فهذا الأمر قد يبدو خادعاً، فإطار (COSO ERM) لديه أهداف واستخدامات مختلفة! فهو ليس مجرد نسخة جديدة ومحسنة أو منقحة من إطار الرقابة الداخلية الصادر عن لجنة المنظمات الراعية (COSO)، فهو أكثر من ذلك بكثير. وتلخص الفقرات التالية هذا الإطار من منظور تحديد مكونات المخاطر ووضع أهداف إدارة المخاطر. إن هدفنا هنا هو تقديم إطار (COSO ERM) مع التركيز على الكيفية التي من خلالها يمكن أن تقوم إدارة المخاطر المؤسسية بتحسين الممارسات الخاصة بحوكمة تقنية المعلومات داخل المؤسسة.

مكونات إطار (COSO ERM): البيئة الداخلية:

كما هو موضح في الشكل التوضيحي (٨-٤)، يوجد عنصر يسمى البيئة الداخلية وُضع في الجزء العلوي من المكونات الخاصة بإطار (COSO ERM). وباستخدام بعض المصطلحات القديمة، فإنه ينظر إلى البيئة الداخلية على أنها بمثابة تتويج إطار (COSO ERM). فبالعودة إلى العصر القديم حيث الجسور المشيدة من الطوب، كان التتويج عبارة عن الحجر الذي يلحم معاً أقواس الطوب التي ترتفع من كل جانب من جانبي الجسر لربط الجسر بأكمله معاً. ويشبه مكون التتويج هذا أيضاً المربع الموجود في الجزء العلوي من الهيكل التنظيمي، حيث يكون الرئيس التنفيذي (CEO) هو الرئيس المعين لهذه الوظيفة. فهذا المستوى هو الذي يعد أساساً لجميع المكونات الأخرى في نموذج إدارة المخاطر المؤسسية الخاص بالمؤسسة ويؤثر في الكيفية التي ينبغي أن يتم من خلالها وضع الإستراتيجيات والأهداف وكيفية هيكلة أنشطة الأعمال المتعلقة بالمخاطر وكيفية تحديد المخاطر واتخاذ إجراءات بشأنها. ويتكون هذا العنصر الذي يمثل الأساس الداخلي لإدارة المخاطر المؤسسية من العناصر التالية:

فلسفة إدارة المخاطر: هي الاتجاهات والمعتقدات المشتركة التي تميز كيف أن المؤسسة تأخذ في الحسبان المخاطر في كل ما تفعله. وعلى الرغم من أن فلسفة إدارة المخاطر ليست في كثير من الأحيان أحد أنواع الرسائل المنشورة في مدونة قواعد السلوك، فإنها تعد أحد

الاتجاهات التي من شأنها السماح لكبار المديرين وغيرهم على جميع المستويات بالرد على اقتراح ما يخص المخاطر المرتفعة من خلال إجابة على غرار "لا، ليس هذا نوعاً من المشروعات التي تهتم به شركتنا". وبالطبع، فإن المؤسسة التي تمتلك فلسفة مختلفة خاصة بها قد ترد على هذا الاقتراح نفسه بإجابة على غرار، "تبدو مثيرة للاهتمام، ما معدل العائد المتوقع؟" في الحقيقة أن كلتا الإجابتين ليستا خاطئتين، لكن يجب على المنشأة أن تحاول تطوير فلسفة واتجاه محدد ومتناغم حول التي تُقبل بها المشاريع المحفوفة بالمخاطر.

الرغبة في المخاطر: مفهوم غير مألوف لدى كثير من المديرين، فالرغبة في المخاطر هي مقدار المخاطرة التي تكون المؤسسة مستعدة لقبولها في سعيها لتحقيق أهدافها. هذه الرغبة في المخاطر يمكن قياسها من حيث الكمية أو النوعية، لكن ينبغي على جميع مستويات الإدارة أن يكون لديها فهم عام لهذا المفهوم وكذلك رغبة في المخاطر المؤسسية بكاملها.

مواقف مجلس الإدارة: لمجلس الإدارة دورٌ مهمٌ جداً في مراقبة بيئة المخاطر للمؤسسة. لذلك يجب على المديرين المستقلين الخارجيين على وجه الخصوص مراجعة الإجراءات الإدارية بعناية، وطرح الأسئلة المناسبة، فهم يمثلون ضوابط الفحص والتوازن بالنسبة للمؤسسة. فعندما يكون أحد مسؤولي المؤسسة الكبار قوياً ولديه توجهٌ يقضي بأن "هذا لا يمكن أن يحدث هنا" عند النظر في المخاطر المحتملة المحيطة ببعض المساعي الجديدة، فإن أعضاء مجلس الإدارة يكونون غالباً هم أفضل من يطرح الأسئلة الصعبة حول الكيفية المتعلقة برد فعل المؤسسة على حدث يقع ولم يكن من المتوقع حدوثه.

النزاهة والقيم الأخلاقية: إن هذا العنصر من عناصر البيئة الداخلية الخاص بإدارة المخاطر المؤسسية (ERM) يحتاج إلى أكثر بكثير من مجرد مدونة قواعد سلوكية منشورة؛ بل إنه يدعو إلى نزاهة سلوك أعضاء المؤسسة وقوة معاييرهم. لذا يلزم وجود ثقافة قوية للشركات لتقوم بتوجيه المؤسسة، على جميع المستويات، في المساعدة على اتخاذ القرارات على أساس المخاطر المتعلقة بها.

الالتزام بالكفاءة: تشير الكفاءة إلى المعرفة والمهارات اللازمة لإنجاز المهام المنوطة. والإدارة هي التي تقرر الكيفية التي يتم بها إنجاز تلك المهام الحرجة المسندة من خلال وضع إستراتيجيات مناسبة وتعيين أفراد مناسبين لأداء هذه المهام الإستراتيجية في أغلب

الأوقات. وقد رأينا جميعاً افتقار المؤسسات لهذا النوع من الالتزام. وتقوم الإدارة العليا بوضع الخطط الكبيرة والمدوية من أجل تحقيق هدف ما، إلا أنها غالباً لا تقوم ببذل أي جهد إيجابي من أجل تحقيق هذا الهدف. ويقوم سوق الأوراق المالية غالباً بفرض عقوبات على مثل هذه الأنشطة.

الهيكل التنظيمي: ينبغي أن يكون لدى الهيكل التنظيمي للمؤسسة خطوط واضحة للسلطة والمسئولية إلى جانب الخطوط الملائمة لتقديم التقارير. إن البنية الضعيفة للهيكل التنظيمي تجعل من الصعب القيام بتخطيط وتنفيذ ورقابة ومتابعة الأنشطة. وقد شهد المهنيون جميعهم الأوضاع التي لم تسمح فيها بنية المؤسسة بتكوين خطوط اتصال مناسبة.

تكاليف السلطة والمسئولية:

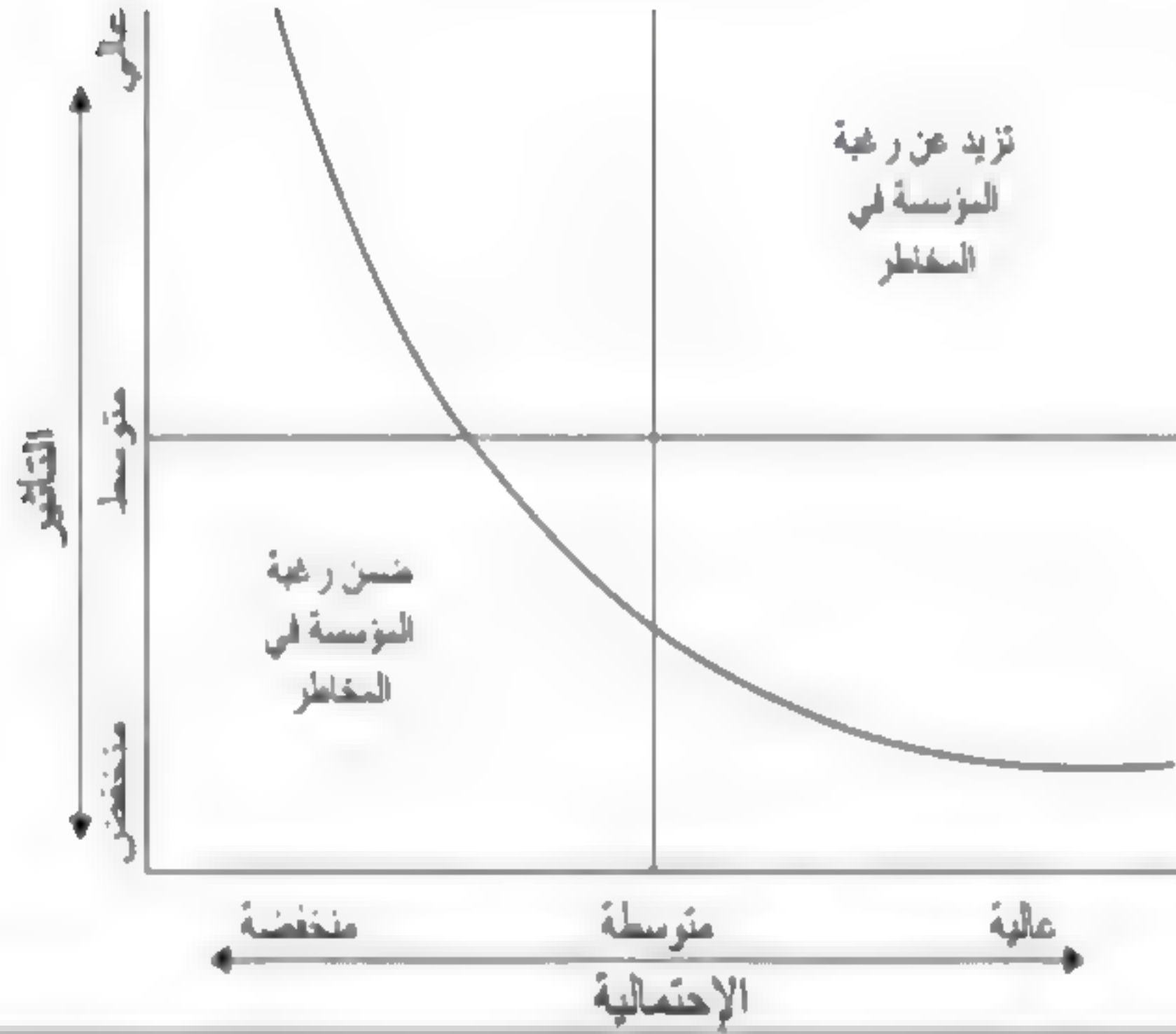
هذا التكليف هو المدى أو الدرجة التي وفقاً لها يتم تكليف مستويات أو شرائح من السلطة والمسئولية أو تفويضها لمجموعات وإدارات مختلفة في المؤسسة. إن الاتجاه السائد اليوم في العديد من المؤسسات هو دفع هذه الأمور مثل مستويات سلطات الموافقة إلى المستويات الدنيا من هيكل المؤسسة، وذلك بإعطاء موظفي الخط الأول التفويض وسلطة الموافقة بشكل أكبر. وثمة اتجاه ذو علاقة وهو "تسطيح" المؤسسات من خلال القضاء على مستويات الإدارة الوسطى. هذه الهياكل المؤسسية تعمل عادة على تعزيز إبداع الموظف وسرعة الاستجابة وزيادة رضا العملاء. وتحتاج هذه النوعية من المؤسسات التي تتعامل وجهاً لوجه مع العملاء إلى إجراءات قوية تحدد "القواعد" لجميع أعضاء طاقم العمل، فضلاً عن متابعة الإدارة المستمرة لهذه الإجراءات حيث يمكن إلغاء قرارات إذا لزم الأمر. كما ينبغي على جميع الأفراد في المؤسسة أن يعرفوا كيفية ترابط أعمالهم وأن يساهموا في تحقيق الأهداف العامة للمؤسسة.

المعايير الخاصة بالموارد البشرية: إن الممارسات التي تتبعها المؤسسة فيما يتعلق بتوظيف وتدريب وتعويض وترقية وتأديب الموظف، وجميع الإجراءات الأخرى، تبعث برسائل إلى جميع أعضاء المؤسسة بشأن ما هو مفضل أو ما هو مسموح به أو ما هو ممنوع. وعندما تقوم الإدارة بغض الطرف عن بعض أنشطة "المنطقة الرمادية" بدلاً من اتخاذ موقف قوي حيالها، فإن هذه الرسالة تصل غالباً بسرعة إلى الآخرين في جميع أنحاء المؤسسة.

إن مكون البيئة الداخلية لإطار (COSO ERM) به اثنان من المخرجات الرئيسية التي تقوم بتغذية العناصر الأخرى في إطار (COSO ERM) وهما: فلسفة إدارة المخاطر في المؤسسة والرغبة النسبية في المخاطر. وبينما ناقشنا فلسفة إدارة المخاطر فيما يتعلق بمواقف مجلس الإدارة وسياسات الموارد البشرية، وأمور أخرى بينهما، فإن الرغبة في المخاطر يكون غالباً المقياس الأكثر مرونة عندما تقرر المؤسسة قبولها لبعض المخاطر ورفضها للبعض الآخر، وذلك تبعاً لاحتمالية حدوثها وتأثيرها. الشكل التوضيحي (٥-٨) يظهر خريطة الرغبة في المخاطر مما يدل على المدى الذي يتعين على المؤسسة وفقاً له قبول المخاطر تبعاً لاحتمالية حدوثها وتأثيرها. وتقول خريطة الرسم البياني هذه أن المؤسسة قد تكون على استعداد للانخراط في مشروع ذي تأثير سلبي عالٍ إذا كان هناك احتمالية منخفضة لحدوثه.

شكل توضيحي (٥-٨)

خريطة الرغبة في المخاطر



كما أن هناك بعداً ثالثاً لهذا المخطط وهو أن المؤسسة في بعض الأحيان يكون لديها رغبة أكبر نحو المساعي المحفوفة بالمخاطر إذا كان هناك إمكانية لتحقيق عائد أعلى.

مكونات إطار (COSO ERM): وضع الهدف:

تم إدراج هذ المكون أسفل مكون البيئة الداخلية من حيث الترتيب، إذ يلخص مكون تحديد الأهداف الخاص بإطار (COSO ERM) بعض الشروط الاستباقية الضرورية التي يلزم توافرها قبل أن تقوم الإدارة بوضع عملية فعالة لإدارة المخاطر في المؤسسة. وبالإضافة إلى البيئة الداخلية المذكورة سابقاً، ينبغي على المؤسسة وضع أهداف عالية المستوى تغطي الأنشطة الخاصة بعمليات التشغيل وإعداد التقارير والامتثال الخاصة بها.

ويدعو إطار (COSO ERM) إلى وضع بيان للمهمة (الرسالة) وهو بيان عام ورسمي للأغراض التي يمكن أن تصبح اللبنة الأولى لتطوير إستراتيجيات وظيفية أكثر تحديداً ويصف غرض المنظمة وأهدافها ومواقفها العامة تجاه المخاطر. وإذا ما تم ذلك بشكل صحيح، فإن بيان المهمة (الرسالة) سيساعد المؤسسة على تحديد سلسلة من أهداف عمليات التشغيل وتطويرها وتنفيذها ورفع تقارير بها وتحقيق مبدأ التوافق في هذا الشأن.

إن مكون البيئة الداخلية لإطار (COSO ERM) الذي سبق الحديث عنه، به اثنان من المخرجات الرئيسية هما: فهم فلسفة إدارة المخاطر في المؤسسة، وتقدير رغبة المؤسسة في المخاطر. هذان المخرجان يسمحان لمكون تحديد الأهداف بتطوير سلسلة من الأهداف للتقليل من المخاطر ولتعريف الرغبة في المخاطرة بشكل رسمي من حيث درجة تحمل المخاطر. ويقصد بدرجة تحمل المخاطر هنا الإرشادات أو المقاييس الرسمية التي يجب أن تستخدمها المؤسسة - على جميع المستويات - لتقدير ما إذا كانت ستقبل المخاطرة أم لا. إن وضع درجة تحمل المخاطر يمكن أن يكون صعباً للغاية بالنسبة للمؤسسات الرسمية. كما ستظهر مشاكل إذا لم تكن القواعد الموضوعية محددة ومعروفة بشكل واضح ومفهومة جيداً ومطبقة بصرامة. وغالباً ما يكون من الصعب تطبيق القواعد، فعلى سبيل المثال، في مارس ٢٠٠٥، قام مجلس إدارة شركة بإعفاء الرئيس التنفيذي للشركة من منصبه بسبب "علاقة عاطفية" مع موظفة^(٣). وكان يتم تجاهل هذا النوع من العلاقات غالباً في الماضي ولكن تم الاعتراف هنا باعتباره انتهاكاً لمدونة قواعد السلوك، واتخذ المجلس إجراءات سريعة وحاسمة حيال ذلك. فإذا كانت المؤسسة تريد إقامة مجموعة صارمة من القواعد، فإنه ينبغي إنفاذها في جميع أنحاء الكيان.

إن أفضل نهج يمكن للمؤسسة اتباعه هو وضع بعض النماذج المقبولة لدرجة تحمل المخاطر. وهذا يعني أنها قد تضع مدى مسموحاً به للمخاطر التي ستقبلها. فعلى سبيل المثال، تجد أن جميع المنتجات التي تأتي من خط الإنتاج قد يكون لها معدلات خطأ مقبولة ومحددة بشكل مسبق وتكون أقل من قيمة معينة. فخط الإنتاج في المؤسسة، على سبيل المثال، قد يرغب في إنتاج سلع بمعدل خطأ لا يزيد عن ٠,٠٠٥ في المئة. وهو معدل خطأ منخفض للغاية في العديد من المجالات، فإدارة الإنتاج في هذه الحالة ستقبل بمخاطر تخص أي مطالبات لضمان المنتج أو أي أضرار قد تلحق بسمعتها إذا وجدت أخطاء ضمن هذه الحدود الضيقة جداً. وبالطبع فإن نطاقات المخاطر في مؤسسة معينة بمنتجات الرعاية الصحية ستكون صارمة إلى أبعد حد.

إن الفكرة الأساسية هنا تتمثل في أنه يجب على المؤسسة أن تحدد إستراتيجياتها وأهدافها المتعلقة بالمخاطر، وفي ظل الإرشادات، يجب أن تقرر المؤسسة مدى رغبتها وتحملها للمخاطر. بمعنى، ما مستوى المخاطر التي تكون المؤسسة على استعداد أن تقبله، وبافتراض وجود تلك القواعد الخاصة بقبول المخاطر، فما هو المقدار الذي تكون على استعداد أن تحيد عنه فيما يخص هذه المقاييس المحددة بشكل مسبق؟ الشكل التوضيحي (٨-٦) يلخص العلاقة بين هذه المكونات الخاصة بتحديد أهداف إطار (COSO ERM) التي يمكن استخدامها لمؤسسة تصنيع متوسطة الحجم. فبدءاً من المهمة الشاملة، يكون النهج عبارة عن (١) وضع الأهداف الإستراتيجية لدعم إنجاز تلك المهمة (٢) وضع إستراتيجية لتحقيق الأهداف (٣) تحديد أي أهداف ذات علاقة و(٤) تحديد الرغبات في المخاطر لاستكمال تلك الإستراتيجية. وقد تم تبني هذا المخطط من المواد الإرشادية المنشورة الخاصة بإطار (COSO ERM)^(٤). ومن أجل إدارة المخاطر على جميع المستويات ومراقبتها، تحتاج المؤسسة إلى تحديد أهدافها وتحديد مدى تحملها للمخاطر عندما تضطر للانخراط في ممارسات محفوفة بالمخاطر ومدى تمسكها بهذه القواعد. ولن تسير الأمور بالشكل السليم إذا ما قامت المؤسسة فقط بتحديد بعض الأهداف المتعلقة بالمخاطر وبعد ذلك تستمر في تجاهلها.

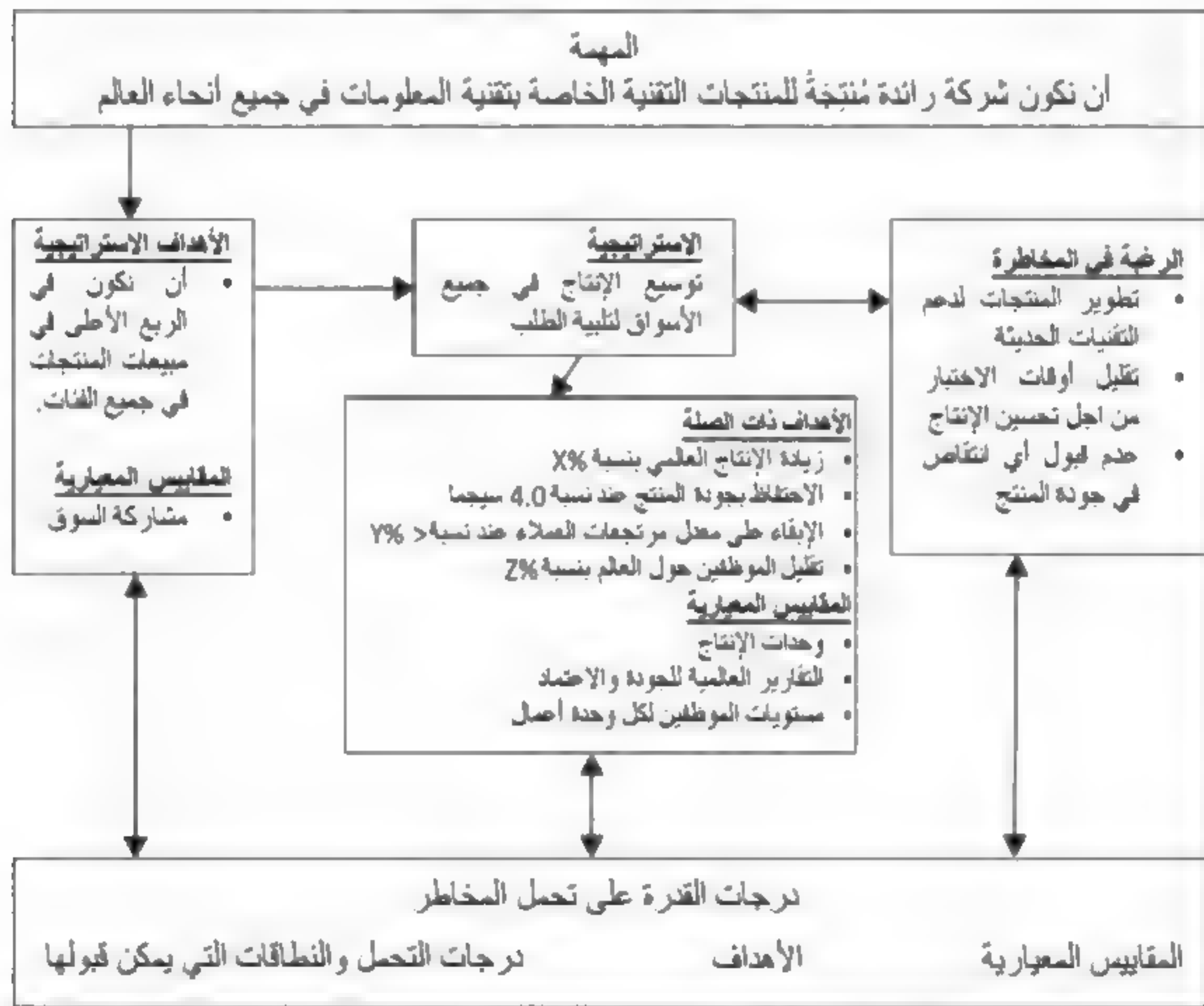
مكونات إطار (COSO ERM): تحديد الحدث:

يقصد بالأحداث الحوادث أو الوقائع الداخلية أو الخارجية في المؤسسة التي تؤثر في تنفيذ إستراتيجية إدارة المخاطر المؤسسية أو تحقيق أهدافها. وبينما يكون الاتجاه السائد

هو التفكير في مثل هذه الأحداث بشكل سلبي (تحديد الخطأ الذي حدث)، فإنه يمكن أن تكون إيجابية أو سلبية أو كليهما. وبالرغم من أن العديد من المؤسسات اليوم تشهد مستوىً قوياً من متابعة الأداء، فإن عملية المتابعة تلك تميل إلى التركيز على مسائل مثل التكاليف والميزانيات وضمان الجودة والامتثال وما شابه ذلك. إن أهداف المخاطر الخاصة بإدارة المخاطر المؤسسية التي سبق الحديث عنها يمكن أن تصبح مفقودة في هذه العملية التي تختص بمتابعة المزيد من الأهداف التشغيلية والأهداف التشغيلية الموجهة نحو العملية بشكل أكبر. وتُطبق المؤسسات في العادة عمليات قوية لمتابعة مثل هذه الأحداث كالتباينات الملائمة في الميزانية وغير الملائمة على وجه الخصوص.

شكل توضيحي (٦-٨)

مكونات وضع أهداف المخاطر في COSO ERM



ومع ذلك ففي كثير من الأحيان لا تكون هناك متابعة منتظمة، سواء للأحداث الفعلية أم للعوامل المؤثرة التي تعد الدافع وراء مثل هذه الأحداث الخاصة بتقلبات الميزانية. وتشمل بعض العوامل المؤثرة التي ينبغي أن تكون جزءاً من عنصر تحديد الأحداث في إطار (COSO ERM) ما يلي:

• **الأحداث الاقتصادية الخارجية:** قد تؤثر الاتجاهات الجارية، قصيرة كانت أم طويلة الأجل، في بعض عناصر الأهداف الإستراتيجية للمؤسسة، ومن ثم يكون لها تأثير في الإطار العام لإدارة المخاطر المؤسسية. ومثال على ذلك الحدث الاقتصادي الخارجي الذي وقع في ٦ مايو ٢٠١٠ والذي شهد فيه أسواق الأسهم الأمريكية والعالمية خسائر فادحة فيما كان يعرف باسم الانهيار السريع (Flash Crash)^(٥). وقد استردت الأسواق عافيتها بسرعة، إلا أن الحدث قد تسبب في قيام العديد باتخاذ إجراءات علاجية متسارعة وكانت غالباً غير مدروسة بشكل جيد. وقد كان هذا الحدث الاقتصادي الخارجي غير متوقع بالمرّة.

• **الكوارث البيئية الطبيعية:** إن العديد من الأحداث، مثل الحرائق أو الفيضانات أو الزلازل، يمكن أن تصبح حوادث أثناء تحديد المخاطر الخاصة بإدارة المخاطر المؤسسية. ويمكن أن تشمل الآثار هنا فقدان إمكانية الوصول إلى بعض المواد الخام الرئيسية، أو أضراراً جسيمة يمكن أن تلحق بالمرافق المادية أو عدم توفر الموظفين.

• **الأحداث السياسية:** قد ينتج عن القوانين واللوائح الجديدة وكذلك نتائج الانتخابات، مخاطر مؤثرة يكون لها تأثيرات ذات صلة بالمخاطر على المؤسسات. ويكون لدى العديد من المؤسسات الكبيرة إدارة خاصة بالشؤون الحكومية تستعرض التطورات والمسااعي المبذولة لإجراء التغييرات. ومع ذلك، فإن مثل هذه الإدارات قد لا تتماشى دائماً مع أهداف إدارة المخاطر المؤسسية.

• **العوامل الاجتماعية:** بينما يكون حدث خارجي مثل الزلزال مفاجئاً ويحدث دون سابق إنذار، فإننا نجد أن معظم التغييرات الخاصة بالعوامل الاجتماعية تكون عبارة عن أحداث تتطور ببطء. وتشمل هذه الأحداث التغييرات الديموغرافية والأعراف الاجتماعية وغيرها من الأحداث التي قد تؤثر في المؤسسات وعملائها مع مرور الوقت. ومثال على التغيير

المجتمعي واقعة الإقالة تلك التي تمت الإشارة إليها سابقاً للرئيس التنفيذي للشركة بسبب علاقة غير شرعية تمت بالتراضي مع موظفة أخرى بالشركة ربما تم تجاهلها لو حدثت في عصر آخر. إلا أن تغير العادات الاجتماعية اليوم هو الذي أدى إلى تلك الإقالة.

• **أحداث البنية التحتية الداخلية:** في كثير من الأحيان تقوم المؤسسات بإجراء تغييرات حميدة من شأنها أن تؤدي إلى أحداث أخرى متعلقة بالمخاطر. فعلى سبيل المثال، التغير في إجراءات خدمة العملاء يمكن أن يسبب شكاوى كبرى وانخفاضاً في رضا العملاء. فالطلب الشديد والمتصاعد على منتج جديد من قبل العملاء قد يؤدي إلى تغييرات في متطلبات الطاقة الاستيعابية للمصنع والحاجة إلى المزيد من الموظفين.

• **الأحداث المتعلقة بالعمليات الداخلية:** على غرار أحداث البنية التحتية يمكن أن تؤدي التغيرات في العمليات الرئيسية إلى وقوع مجموعة كبيرة من الأحداث المتعلقة بتحديد المخاطر. وكما هو الحال بالنسبة للعديد من هذه العناصر، فإن تحديد المخاطر قد لا يكون فورياً، وقد يمر بعض الوقت قبل أن تشير الأحداث المتعلقة بالعملية إلى الحاجة إلى تحديد المخاطر.

• **الأحداث التقنية الخارجية والداخلية:** تواجه جميع المؤسسات الكثير من الأحداث التقنية المتواصلة التي يمكن أن تؤدي إلى الحاجة إلى تحديد رسمي للمخاطر، فبعضها يتم تدريجياً مع مرور الوقت في حين أن البعض الآخر يكون مفاجئاً بشكل كبير. فقد كانت الشبكة العنكبوتية العالمية لوقت ما قيد استخدامنا، إلا أن التحول إلى بيئة الإنترنت بالنسبة للكثيرين تم بشكل تدريجي إلى حد ما. وفي حالات أخرى، فإن التوسع في نظم حوسبة الشبكات الاجتماعية التي تم الحديث عنها في الفصل الحادي والعشرين من هذا الكتاب كان له تأثير كبير في المؤسسات من حيث العلاقات مع أصحاب المصلحة لدى المؤسسة وسمعتهم.

تحتاج أي مؤسسة إلى تعريف واضح لما تراه عبارة عن أحداث هامة للمخاطر، ومن ثم يجب أن يكون لديها عمليات مطبقة لمتابعة كل أحداث المخاطر الهامة المحتملة المتنوعة تلك، وعلى هذا يمكن للمؤسسة أن تتخذ الإجراءات المناسبة. وفي الواقع يعد هذا أحد أنواع التفكير الواعد لعملية تكون غالباً صعبة الإدراك داخل العديد من المؤسسات.

إن عملية النظر في مختلف الأحداث الداخلية والخارجية المحتملة للمخاطر واتخاذ قرار بشأن أي من هذه الأحداث يتطلب مزيداً من الاهتمام وقد يكون أمراً صعباً، لكن إطار (COSO ERM) يقدم هنا بعض المساعدة فهو يقترح أن تقوم المؤسسة بوضع بعض العمليات الرسمية لمراجعة المخاطر الهامة المحتملة ومن ثم تبدأ عملية اتخاذ الإجراء. وتبعاً لإرشادات إطار (COSO ERM)، فإن المؤسسة قد تأخذ بعين الاعتبار بعضاً من الأساليب التالية:

- **مستودعات الأحداث:** ينبغي على إدارة المؤسسة أن تراجع الأحداث الأخرى المتعلقة بالمخاطر الشائع حدوثها في الصناعة أو في مجال وظيفي معين لإحدى المؤسسات. بمعنى أنه يجب على المؤسسة أن تنظر في إنشاء أرشيف مصدري لـ "الدروس المستفادة". ويعد هذا نوعاً من أنواع البيانات التاريخية التي تم الحصول عليها عن طريق أعضاء في المؤسسة طالت مدد بقائهم فيها، ويمكنهم تقديم أنواع من التعليقات مثل "لقد جربنا ذلك منذ عدة سنوات، ولكن...". إن هذا النوع من التأريخ في كثير من الأحيان يكون غير موجود في مؤسسات اليوم، غير أن الإدارة الفعالة لإدارة المخاطر يمكن أن توفر بعض المساعدة في هذا المقام.
- **ورش العمل الميسرة:** يمكن للمؤسسة أن تعقد ورش عمل للعديد من الإدارات لتناقش بدايةً العوامل المحتملة للمخاطر التي يمكن أن تكون نتيجة للأحداث الداخلية أو الخارجية المتنوعة ومن ثم تقوم بتطوير خطط عمل لتصحيح المخاطر المحتملة. يعد هذا أحد الأساليب المقترحة التي تبدو جيدة، لكن جرت العادة بالنسبة للعديد من المؤسسات أنها لا تقوم بتخصيص جزء من أوقاتها الثمينة لمقابلة مجموعات من مختلف الإدارات للحديث عن المخاطر باستخدام صيغة من نوع "ماذا سيحدث لو..".
- **مقابلات واستبيانات واستطلاعات:** إن المعلومات التي تخص أحداث المخاطر المحتملة يمكن أن تأتي من مجموعة واسعة من المصادر. مثل التعليقات على خطابات رضا العملاء، والتعليقات التي تأتي من نظم وسائل التواصل الاجتماعي. أو التعليقات الصادرة من المقابلات النهائية مع الموظفين التاركن لوظائفهم. وهناك حاجة للحصول على المعلومات وتصنيفها من أجل تحديد أي منها يمكن اعتباره مؤشراً على وجود أحداث مخاطر. وهذه الأنواع من الردود ستساعد على بناء ثقافة إدارة المخاطر المؤسسية.

- **تحليل تدفق أو سير العمليات:** إن المواد الخاصة بدعم تقنيات تطبيق إطار (COSO ERM) توصي باستخدام مخططات التدفق لمراجعة العمليات وتحديد الأحداث المحتملة للمخاطر، وبالنسبة للعديد من المؤسسات فإن مخططات تدفق العملية تتشابه إلى حد بعيد مع وثائق الرقابة الداخلية التي كان ينبغي إعدادها وتحديثها باعتبارها جزءاً من أعمال التوثيق الخاصة بالبند ٤٠٤ من قوانين ساربينز- أوكسلي SOX، حيث يتم تحديد الضوابط الداخلية وأي نقطة من نقاط الضعف الموجودة في العملية الرقابية. وقد تم مناقشة هذه العمليات في الفصل الثاني من هذا الكتاب الخاص بقانون ساربينز أوكسلي.
- **الأحداث الرائدة ومحفزات التصعيد:** يجب على إدارة المؤسسة أن تقوم بوضع سلسلة من الأهداف الخاصة بوحدة الأعمال، ولا شك أن معايير القياس ضرورية لتحقيق تلك الأهداف، فمعايير درجة تحمل المخاطر تكون ضرورية لتعزيز الإجراءات التصحيحية. فعلى سبيل المثال، قد تقوم مجموعة تقنية المعلومات في المؤسسة بوضع هدف للحفاظ على الضوابط الأمنية المعززة بشأن التهديدات الهجومية لاختراق شبكة تقنية المعلومات. وبقياس عدد محاولات الاقتحام التي تم تحديدها خلال فترة معينة، وجدنا أن عتبة threshold ذلك تجاوزت ربما ثلاث تدخلات في شهر معين، مما أدى إلى اتخاذ مزيد من الإجراءات. وتوجد اليوم أدوات برمجية جيدة جداً متاحة تسمى لوحات المعلومات^(٦) dashboards لمتابعة الأداء الخاص بجوانب المؤسسة، وفي الغالب تكون معقدة للغاية. هذه التطبيقات تعمل على نحو مماثل عمل التحكم على لوحة العدادات في السيارة، إذ إن المؤشرات تعطي إشارات ضوئية في ظروف معينة مثل انخفاض ضغط الزيت أو ارتفاع درجة حرارة المحرك. والفكرة هي أن يُقدم تقرير عن حالة المخاطر من خلال رسومات بسيطة، سهلة الفهم إلى حد ما مثل الأسهم العلوية أو السفلية أو شعارات إشارة المرور الشائعة الحمراء والصفراء والخضراء.
- **تتبع بيانات أحداث الخسارة:** في حين أن أسلوب لوحة المعلومات يقدم فقط متابعات لأحداث المخاطر وقت حدوثها، فإنه يكون من المفيد غالباً وضع الأمور في نصابها بعد مرور بعض الوقت. ويشير تتبع حادث الخسارة إلى استخدام كل من مصادر قاعدة البيانات الداخلية والعامة لتتبع النشاط في المجالات ذات الاهتمام. ويمكن لهذه المصادر

أن تغطي مجموعة واسعة من المجالات بدءاً من قيادة المؤشرات الاقتصادية إلى أن تصل إلى معدلات فشل المعدات الداخلية. ومرة أخرى، يجب على المنشأة تثبيت عمليات فعالة لتحديد المخاطر بهدف تتبع كل من الأحداث الداخلية والخارجية المتعلقة بالمخاطر.

إن أدوات وأساليب تحديد المخاطر التي تمت مناقشتها للتو يمكن أن تسفر عن بعض المعلومات القيمة جداً والمفيدة للمؤسسة، والتي تحدد إما المخاطر وإما الفرص أو الاثنين معاً. إن الحل يكمن في الحاجة إلى تحليلات جيدة للبيانات، فضلاً عن الشروع في خطط عمل، سواء للحماية من المخاطر أو للاستفادة من الفرص المحتملة.

مكونات إطار (COSO ERM): تقييم المخاطر:

تحدثنا عن مكون البيئة الداخلية باعتباره تتويجاً أو حجر زاوية لإطار (COSO ERM)، مع مكون المتابعة باعتباره عنصراً أساسياً لدعم الإطار. ويقع عنصر تقييم المخاطر تقريباً في وسط الإطار ويمثل جوهر إطار (COSO ERM). كما يسمح مكون تقييم المخاطر للمؤسسة بالنظر في الأثر المحتمل للأحداث المرتبطة بالمخاطر المحتملة على إنجاز المؤسسة لأهدافها. ويجب تقييم هذه المخاطر من منظورين: احتمالية حدوث المخاطر، وتأثيرها المحتمل. وكجزء أساسي لعملية تقييم المخاطر هذه، تحتاج الإدارة أيضاً إلى أن تنظر في مفهومين أساسيين: المخاطر المتأصلة والمخاطر المتبقية.

١- **المخاطر المتأصلة (الكامنة):** كما حددها مكتب الحكومة الأمريكية للإدارة والميزانية، فإن المخاطر المتأصلة هي "إمكانية هدر أو فقدان أو استخدام غير مصرح به أو اختلاس أو استغلال بسبب طبيعة النشاط نفسه". والعوامل الرئيسية التي تؤثر في المخاطر المتأصلة في أي نشاط داخل الشركة هي حجم ميزانيتها وقوة إدارة المجموعة وحنكتها وبساطة الطبيعة الأصلية لأنشطتها. وتكون المخاطر المتأصلة خارجة عن سيطرة الإدارة ونابعة عادة من العوامل الخارجية. فعلى سبيل المثال، متاجر التجزئة الرئيسية وول مارت Walmart كبيرة جداً ومهيمنة على أسواقها ويواجهها مستوى معين من مختلف المخاطر المتأصلة بسبب حجمها الهائل.

٢- المخاطر المتبقية: هي تلك المخاطر التي تبقى بعد استجابة الإدارة لتهديدات المخاطر وتطبيق الإجراءات المضادة. ويوجد دائماً مستوى ما من المخاطر المتبقية.

يدل هذان المفهومان على أن إدارة المؤسسة ستواجه دائماً بعض المخاطر. فبعد أن تقوم المؤسسة بمعالجة المخاطر التي خرجت من عملية تحديد المخاطر، فإنها تظل تواجه بعض المخاطر المتبقية التي يلزم علاجها لاحقاً، كالعديد من المخاطر المتأصلة القليلة التأثير. وول مارت، على سبيل المثال، يمكن أن تتخذ بعض الخطوات للحد من المخاطر المتأصلة المتعلقة بهيمنة السوق. لكنها لا يمكن أن تفعل شيئاً أساسياً بشأن المخاطر المتأصلة (الكامنة) لزلاز طبعي كبير في منطقة عمليات التشغيل.

إن الاحتمالية والتأثير هما أيضاً مكونان رئيسيان آخران ضروريان لتقييم المخاطر. فالاحتمالية هي إمكانية حدوث مخاطرة ما، وتوصف غالباً بأنها احتمال مرتفع أو احتمال متوسط أو احتمال منخفض للمخاطر التي تحدث. وتوجد بعض الأدوات الكمية الجيدة هنا كذلك، لكنها غير مجدية كثيراً في تقدير احتمالية حدوث المخاطرة من حيث العلامة العشرية المتعددة إذا لم يكن هناك أي أساس لتطوير ذلك العدد الدقيق إلى ما هو أبعد من الحسابات الإحصائية الاعتيادية.

إن تقدير التأثير في حالة حدوث المخاطرة يعتبر أسهل بعض الشيء. فيمكن أن تقوم المؤسسة بوضع بعض التقديرات الدقيقة نسبياً لأمر مثل تكلفة استبدال المرافق والمعدات، تكلفة استعادة نظام معين، وإلى حد ما تكلفة الفرص التجارية الضائعة (الأعمال الخاسرة) بسبب العطل. وعلى كل حال، فإن المفهوم الشامل وراء إدارة المخاطر المؤسسية (ERM) ليس تطوير حسابات دقيقة وحسابات على المستوى الاكتواري فيما يخص المخاطر لكن للحصول على مقياس معين لتوفير إطار فعال لإدارة المخاطر. ويمكن تطوير تحليل احتماليات المخاطر والتأثيرات المحتملة من خلال سلسلة من المقاييس النوعية والكمية. فالفكرة الأساسية هي تقييم جميع المخاطر التي تم تحديدها وتصنيفها من حيث الاحتمالية والتأثير بطريقة متناغمة.

مكونات إطار (COSO ERM): الاستجابة للمخاطر:

إن الخطوة التالية بعد تقييم المزيد من المخاطر الهامة وتحديدتها، هي تحديد كيفية الاستجابة لمختلف هذه المخاطر التي تم تحديدتها. وتعد هذه من المسؤوليات الإدارية،

فالإدارة هي التي تقوم بإجراء مراجعة دقيقة لاحتمالات المخاطر المقدرة وتأثيراتها المحتملة، كما أنها تأخذ في الاعتبار التكاليف والفوائد المرتبطة بها. ولوضع إستراتيجيات ملائمة للاستجابة للمخاطر يتم اتباع أي أسلوب من الأساليب الأربعة الأساسية:

١- **التفادي (التجنب):** إستراتيجية تعتمد البعد عن المخاطر، مثل بيع أحد وحدات الأعمال التي يمكن أن تؤدي إلى مخاطرة أو الخروج من منطقة جغرافية محل قلق. وتكمن صعوبة تطبيق هذه الإستراتيجية في أن المؤسسات في كثير من الأحيان لا تتخلى عن المنتج أو تبتعد عن المخاطر إلا بعد أن يقع الحدث الخاص بالمخاطرة. فإذا لم تكن هناك رغبة في المخاطر حتى وإن كانت منخفضة للغاية، فمن الصعب الابتعاد عن منطقة العمل أو خط الإنتاج بسبب ظهور مخاطر محتملة في المستقبل، هذا إذا ما كان كل شيء في الوقت الحاضر يسير على ما يرام في نواح أخرى. وقد تكون إستراتيجية التفادي مكلفة إذا كانت الاستثمارات قد اعتمدت للدخول في منطقة مرتبطة بحدوث انسحاب تبقي لتجنب المخاطر.

٢- **التخفيف:** قد تكون قرارات الأعمال قادرة على الحد من مخاطر معينة. فتنويع المنتجات قد يقلل من مخاطر الاعتماد القوي للغاية على خط إنتاج واحد رئيسي. كما أن تقسيم مركز عمليات تشغيل تقنية المعلومات إلى موقعين منفصلين جغرافياً سيقلل من مخاطر بعض الأعطال الكارثية. وتوجد مجموعة واسعة من الإستراتيجيات الفعالة في كثير من الأحيان للحد من المخاطر على جميع المستويات التي تنزل بها إلى المرحلة الدنيا، لكنها تكون مهمة من الناحية العملية لموظفي التدريب المتعدد التخصصات.

٣- **المشاركة:** تتقاسم جميع المؤسسات تقريباً وكذلك الأفراد بصورة منتظمة بعض مخاطرها من خلال شراء التأمين لتطويق تلك المخاطر أو مشاركتها. وهناك العديد من التقنيات الأخرى المتوفرة هنا كذلك. فبالنسبة للمعاملات المالية، فإن المؤسسة يمكن أن تنخرط في العمليات التحوطية للحماية من تقلبات الأسعار المحتملة. ومن الأمثلة الشائعة على التطويق هو استخدام المستثمر لخيارات البيع أو الطلب لتغطية التحركات القوية للأسعار. كما يمكن مشاركة المخاطر والمزايا المحتملة للأعمال من خلال اتفاقيات مشتركة.

٤- القبول: ويقصد بها إستراتيجية اللاإجراء. فمثلاً عندما يكون لدى المؤسسة "تأمين ذاتي" ضد بعض المخاطر، فبدلاً من شراء وثيقة تأمين في الأساس، يجب على المؤسسة أن تنظر في احتمالية المخاطرة وأثرها في ضوء تحمل المخاطر الموضوعة، وبعد ذلك تقرر ما إذا كانت ستقبل هذه المخاطرة أم لا. ونظراً لكثرة المخاطر وتنوعها، يمكن أن يكون هذا هو نهج المؤسسة، فالقبول غالباً ما يشكل إستراتيجية ملائمة لبعض المخاطر.

وينبغي على الإدارة وضع إستراتيجية عامة للاستجابة لكل مخاطرة من مخاطرها باستخدام نهج قائم على أحد هذه الإستراتيجيات الأربع العامة. وللقيام بذلك، ينبغي النظر في التكاليف مقابل الفوائد الناتجة عن كل استجابة للمخاطر المحتملة لمواءمتها بشكل أفضل مع الرغبة في المخاطر الإجمالية للمؤسسة. فمثلاً، إدراك المؤسسة بأن تأثير مخاطرة معينة يكون منخفضاً نسبياً سيتم موازنته مقابل درجة تحمل منخفضة للمخاطرة، وهذا يشير بدوره إلى أن التأمين يجب شراؤه لتوفير الاستجابة للمخاطر المحتملة. وبالنسبة لكثير من المخاطر، فإن الاستجابات المناسبة تكون واضحة ومفهومة تقريباً للجميع. فعملية تشغيل تقنية المعلومات، على سبيل المثال. ينبغي أن تستهلك الوقت والموارد لإجراء نسخ احتياطية لملفات البيانات الرئيسية وتنفيذ خطة استمرارية العمل.

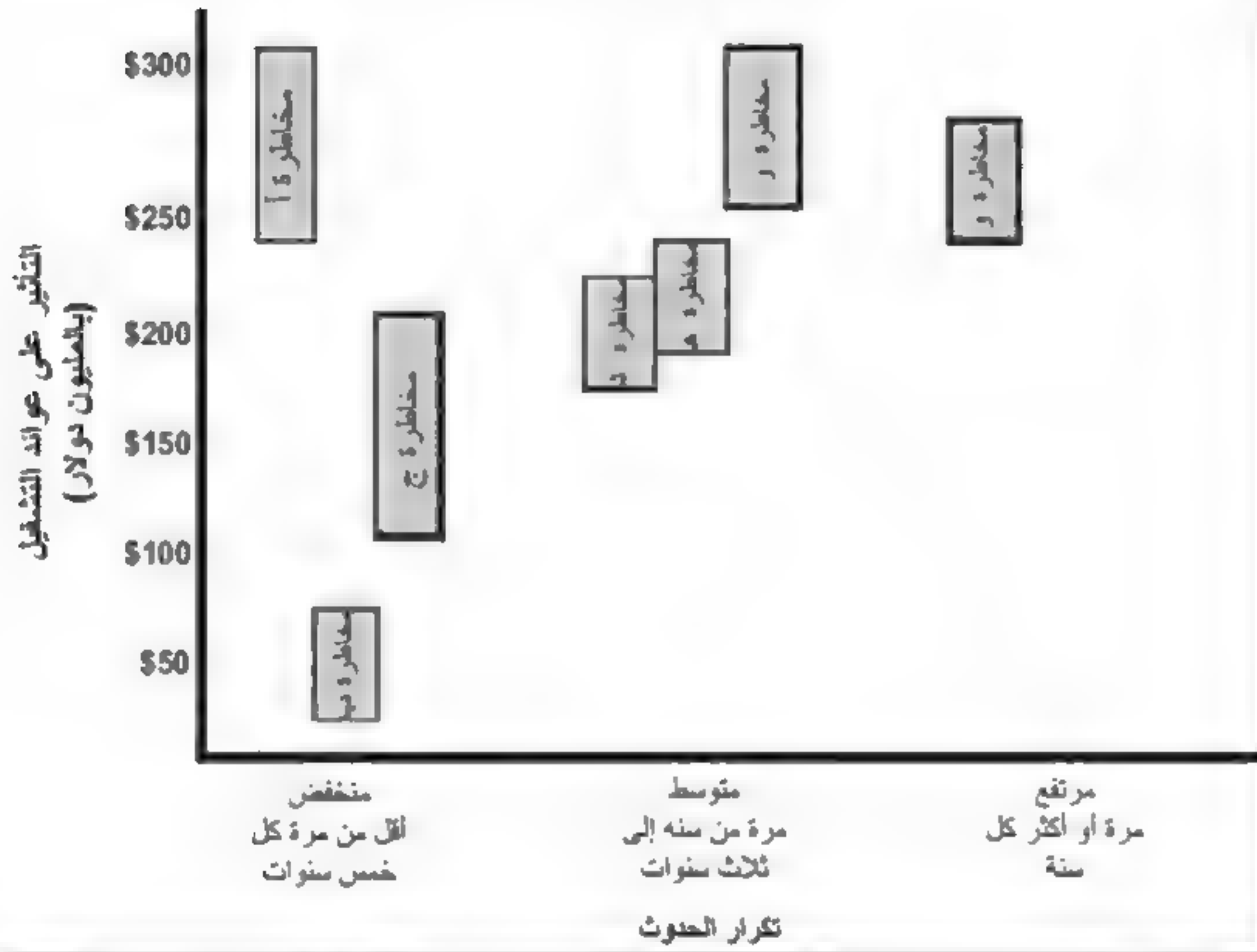
إن المؤسسة، عند هذه النقطة، يجب أن تعود إلى الأهداف العديدة للمخاطر التي تم وضعها وكذلك نطاقات تحمل تلك الأهداف. ومن ثم ينبغي أن تعيد مناقشة كل من الاحتمالية والتأثير المرتبطين بكل مخاطرة من المخاطر التي تم تحديدها ضمن أهداف المخاطر تلك لوضع تقييم لكل من هذين الصنفين للمخاطر. كما يلزم إجراء تقييم شامل لاستجابات المخاطر المخطط لها وكيفية مواءمة تلك المخاطر مع درجات التحمل الكلية لمخاطر المؤسسة. وعند هذه النقطة في عملية تقييم المخاطر، يتعين على المؤسسة أن تُقيّم الاحتمالية والتأثير المحتمل لكل من المخاطر المحيطة بأهدافها، وكذلك بعض التقديرات لكل منهما. وتقوم بالخطوة التالية المتمثلة في تطوير مجموعة من استجابات المخاطر المحتملة. ولعل هذه هي أصعب خطوة في بناء إطار برنامج فعال لإطار (COSO ERM). فمن السهل نسبياً

تحديد خمسة في المئة من احتمالية مخاطر وقوع حريق في حاوية نفايات، ومن ثم وضع الخطوط العريضة للاستجابة للمخاطر كتثبيت طفاية حريق في مكان قريب. ومع ذلك، فإن الاستجابات لمعظم المخاطر تكون أكثر تعقيداً وتتطلب خطاً تفصيلية إلى حد ما للاستجابة للمخاطر.

ويجب على المؤسسة في البداية استعراض جميع مخاطرها الرئيسية المحددة ذات التأثير العالي والاحتمالية العالية ووضع سلسلة من خطط الاستجابة للمخاطر. وعلى أية حال، قد تكون هذه عملية إدارية صعبة. وعلى الرغم من أنها قد تكون سهلة نسبياً، كاتباع مثالنا السابق، الخاص بتثبيت طفاية حريق لتوفير الحماية من حرائق حاوية نفايات، فإن الأمور لا تكون عادة بهذه البساطة. والنقطة الأساسية هنا تتضح في أن عملية تطوير عمليات الاستجابة للمخاطر في حد ذاتها تتطلب قدراً كبيراً من التخطيط والتفكير الإستراتيجي. إن البدائل العديدة والمختلفة للاستجابة للمخاطر تنطوي على التكاليف والوقت والتخطيط التفصيلي للمشروع. وبالإضافة إلى التخطيط والتفكير الإستراتيجي، فإن هذه العملية الخاصة بتخطيط الاستجابة للمخاطر تتطلب مساهمة إدارية كبيرة والموافقة على التعرف على مختلف الاستجابات البديلة للمخاطر ووضع خطط عمل موضع تنفيذ لتحقيق الاستجابات المناسبة. ويدعو إطار (COSO ERM) إلى مواجهة المخاطر التي يتعين النظر فيها وتقييمها على مستوى الكيان أو على مستوى المحفظة وتقييمها وتقديرها لكل وحدة من وحدات العمل الفردية أو تقسيمها حسب الإدارة أو حسب الوظيفة وأساليب مماثلة للنظر في مخاطر المؤسسة. وينبغي بعد ذلك تلخيص المخاطر بناءً على أثرها وتكرار حدوثها. وكما هو مبين في الشكل التوضيحي (٨-٧)، يعد هذا أحد أنواع الاتصالات المستخدمة الذي من شأنه أن يساعد الإدارة العليا ومجلس الإدارة في فهم محفظة من المخاطر التي تواجه المؤسسة.

شكل توضيحي (٧-٨)

عرض محفظة ملخص المخاطر



مكونات إطار (COSO ERM): أنشطة الرقابة:

إن الأنشطة الرقابية لإطار (COSO ERM) هي السياسات والإجراءات اللازمة لضمان تنفيذ الاستجابات للمخاطر التي تم تحديدها. وعلى الرغم من أن بعض هذه الأنشطة قد تكون مرتبطة فقط بالاستجابة للمخاطر التي تم تحديدها والمخاطر المقبولة في منطقة واحدة من المؤسسة، فإنها تتداخل غالباً من خلال الإدارات والوحدات المتعددة. ويجب أن ترتبط أنشطة الرقابة الخاصة بإطار (COSO ERM) بشكل وثيق مع عنصر الاستجابة للمخاطر الذي سبق مناقشته.

وبعد أن يتم اختيار الاستجابات المناسبة للمخاطر، يجب على إدارة المؤسسة اختيار أنشطة الرقابة الضرورية لضمان أن استجابات المخاطر تلك يتم تنفيذها في الوقت المناسب

وبطريقة فعالة. إن عملية مراجعة مدى صحة تنفيذ أنشطة الرقابة في العادة تكون مشابهة جداً للعمليات التي تُمارس على أنها جزء من البند ٤٠٤ من قوانين SOx الخاص بتقييمات الرقابة الداخلية^(٧) التي تم الحديث عنها في الفصل الثاني من هذا الكتاب. ويمكن تنفيذ أنشطة الاستجابة للمخاطر الخاصة بإطار (COSO ERM) بالخطوات التالية:

١- تحقيق فهم قوي للمخاطر المؤثرة التي تم تحديدها ووضع إجراءات رقابية لمتابعة تلك المخاطر أو تصحيحها.

٢- وضع إجراءات اختبارية لتحديد ما إذا كانت تلك الإجراءات الرقابية المتعلقة بالمخاطر تعمل على نحو فعال أم لا.

٣- أداء اختبارات لإجراءات الرقابة لتحديد ما إذا كانت عملية متابعة المخاطر التي تم اختبارها تعمل بشكل فعال وكما هو متوقع أم لا.

٤- إجراء التعديلات أو التحسينات الضرورية لتحسين عمليات متابعة المخاطر.

هذه العملية ذات الخطوات الأربع هي في الأساس ما تخضع له المؤسسات من متطلبات قانون SOx التي كانت تقوم بمراجعة عمليات الرقابة الداخلية لديها واختبارها والتأكد على أنها تعمل بشكل مناسب. ويوجد فرق رئيسي هنا مضمونه أن المؤسسة مطالبة بشكل قانوني بالامتثال لإجراءات قانون SOx من أجل التأكيد على ملاءمة ضوابطها الداخلية لمدققها الخارجيين. ولا توجد مثل هذه المتطلبات القانونية مع إطار (COSO ERM). وينبغي أن تسعى المؤسسة لتثبيت أنشطة رقابية لمتابعة المخاطر من أجل تقييم المخاطر المختلفة التي قامت بتحديدتها. وبسبب الطبيعة الحساسة للعديد من المخاطر التي تتعرض لها المؤسسة، فإن المتابعة الإدارية للمخاطر تكون حساسة جداً بالنسبة للسلامة العامة للمؤسسة نظراً لطبيعة المخاطر المختلفة التي قد تواجهها.

إن العديد من الأنشطة الرقابية المندرجة تحت الضوابط الداخلية الصادرة عن لجنة المنظمات الراعية (COSO) تكون سهلة التحديد والاختبار إلى حد ما نظراً للطبيعة المحاسبية بالنسبة للكثيرين، وهي بشكل عام تشمل ما يلي:

- **فصل المهام:** إن المفهوم الأساسي للرقابة هو أن الشخص الذي يبدأ المعاملة لا ينبغي أن يكون هو الشخص نفسه الذي يقوم باعتماد تلك المعاملة.
- **مسارات التدقيق:** ينبغي تنظيم العمليات، فمثل هذه النتائج النهائية يمكن أن تعزى بسهولة إلى المعاملات التي تكون قد تسببت في وجود تلك النتائج.
- **الأمن والسلامة:** يجب أن يكون لعمليات الرقابة إجراءات رقابية مناسبة، وفي مثل هذه الحالة يمكن للأشخاص المخولين فقط مراجعتها أو تعديلها.
- **التوثيق:** يجب أن تكون العمليات موثقة بشكل مناسب.

إن تلك الإجراءات الرقابية، وغيرها، يسهل استيعابها بشكل جيد إلى حد ما، وتقبل التطبيق على جميع عمليات الرقابة الداخلية المعمول بها في المؤسسة، كما أنها تنطبق إلى حد ما على كثير من الأحداث المتعلقة بالمخاطر. فالعديد من كبار المديرين يمكنهم بسهولة تحديد بعض الضوابط الأساسية اللازمة في العديد من عمليات الأعمال. فعلى سبيل المثال، إذا طلب منهم تحديد نوعيات معينة من الضوابط الداخلية التي ينبغي أن تُبنى داخل نظام تقنية المعلومات الخاص بحسابات المدفوعات، فإن العديد من المهنيين سيقومون بتحديد نقاط رقابة هامة كوجوب اعتماد الشيكات الصادرة من النظام من قبل عدة أشخاص، كما يجب أن تكون السجلات المحاسبية في موضع التنفيذ لتتبع الشيكات الصادرة، كما ينبغي أن تكون عملية إصدار الشيك للأشخاص المخولين فقط ممن يمكنهم بدء مثل هذه المعاملات المالية. وتعد هذه بشكل عام إجراءات الرقابة المفهومة جيداً وعلى نطاق واسع. وتواجه المؤسسة غالباً مهمة أكثر صعوبة في تحديد أنشطة الرقابة لدعم إطار إدارة المخاطر المؤسسية الخاص بها.

وكما تحدثنا سابقاً، فكجزء من مكون تحديد أحداث إدارة المخاطر المؤسسية (ERM)، فإن الإدارة تحتاج إلى التفكير في فئات المخاطر هذه من حيث مجالات المخاطر الرئيسية لعمليات التشغيل، مثل الإيرادات والشراء وإنفاق رأس المال، ونظم المعلومات. كما يمكن تعريف أنشطة رقابية بعينها تتعلق بالمخاطر داخل كل فئة من هذه الفئات، سواء للمؤسسة بأكملها أم التي تغطي وحدة أو إدارة ما. وبالرغم من عدم وجود مجموعة من الأنشطة الرقابية المقبولة أو المعيارية الموحدة لإدارة المخاطر المؤسسية حتى هذا الوقت، فإن وثائق إطار (COSO ERM) تشير إلى عدة مجالات على النحو التالي:

- **مراجعات المستوى الأعلى:** بينما تكون الإدارة العليا غافلة إلى حد ما عن إجراءات الرقابة الداخلية الخاصة بـ "هل الحسابات المدينة تساوي الحسابات الدائنة؟" التي تغطيها فرق ومدققو الحسابات المالية لديها، فإنهم يجب أن يكونوا على علم تام بأحداث المخاطر التي تم تحديدها داخل الوحدات التنظيمية، وينبغي إجراء مراجعات بصورة منتظمة وعلى مستوى عالٍ حول وضع المخاطر التي تم تحديدها وكذلك التقدم المحرز في استجابات المخاطر. هذا النوع من المراجعة المنتظمة إلى جانب الإجراءات التصحيحية المناسبة العالية المستوى يُعد نشاط الرقابة الرئيسي لإدارة المخاطر المؤسسية.
- **الإدارة الفنية أو الوظيفية المباشرة:** بالإضافة إلى المراجعات ذات المستوى الأعلى المذكورة، فإنه ينبغي أن يكون لمديري الوحدات الوظيفية والوحدات المباشرة دور رئيسي في متابعة الأنشطة الرقابية للمخاطر. وهذا أمر مهم ولا سيما في المؤسسات الكبيرة والمتنوعة حيث لا يجب أن تتم الأنشطة الرقابية على مستوى وحدة محلية فحسب، ومن ثم دفع الهرم التنظيمي إلى مستوى إدارة مركزية معينة. وبدلاً من ذلك، يجب أن تتم أنشطة الرقابة ذات الصلة بالمخاطر في إطار وحدات تشغيل منفصلة، في ظل اتصالات وحلول المخاطر التي تقع عبر قنوات المؤسسة.
- **معالجة المعلومات:** سواء كانت عمليات نظم تقنية معلومات أم أشكالاً أكثر بساطة كورقة أو رسائل، فإن إجراءات معالجة المعلومات تمثل عنصراً أساسياً في الأنشطة الرقابية المتعلقة بالمخاطر الخاصة بالمؤسسة. إن إجراءات الرقابة المناسبة هنا، مع التركيز على عمليات تقنية المعلومات للمؤسسة ومخاطرها، تم الحديث عنها بمزيد من التفصيل في الفصل الرابع عشر من هذا الكتاب حول تطبيق النظم المتكاملة.
- **الضوابط المادية:** يوجد العديد من الأحداث المتعلقة بالمخاطر تشتمل على أصول مادية كالمعدات والمخزون والأوراق المالية، ومرافق مادية كمصنع. وسواء كانت هذه الإجراءات المادية تتعلق بالجرد أم بعمليات التفتيش أو أمن أحد المصانع، فإنه يجب على المؤسسة أن تضع إجراءات ملائمة للأنشطة الرقابية المادية القائمة على المخاطر.
- **مؤشرات الأداء:** توظف المؤسسة الحديثة النموذجية اليوم مجموعة واسعة من أدوات إعداد التقارير المالية والتشغيلية. ويمكن استخدام العديد من هذه الأدوات كما هي

أو بعد التعديل عليها لدعم إعداد تقارير الأداء المرتبطة بأحداث المخاطر. وفي كثير من الحالات، يمكن تعديل أدوات الأداء الكلي للمؤسسة لدعم هذا المكون المهم للنشاط الرقابي.

• **الفصل بين المهام:** هذا هو النشاط الرقابي التقليدي، سواء كان للضوابط الداخلية لإجراءات العمل أو إدارة المخاطر. فالشخص الذي يبدأ إجراءات معينة لا ينبغي أن يكون هو الشخص نفسه الذي يجيز أو يوافق على تلك الإجراءات. هذا النشاط الرقابي الرئيسي مهم، سواء كان ذلك في وحدة أعمال صغيرة يُطلب فيها من مشرف الموظف أن يفحص ويوافق على إجراءات الموظف أم من خلال الرئيس التنفيذي الذي يجب أن يحصل على الموافقة الرقابية من مجلس الإدارة.

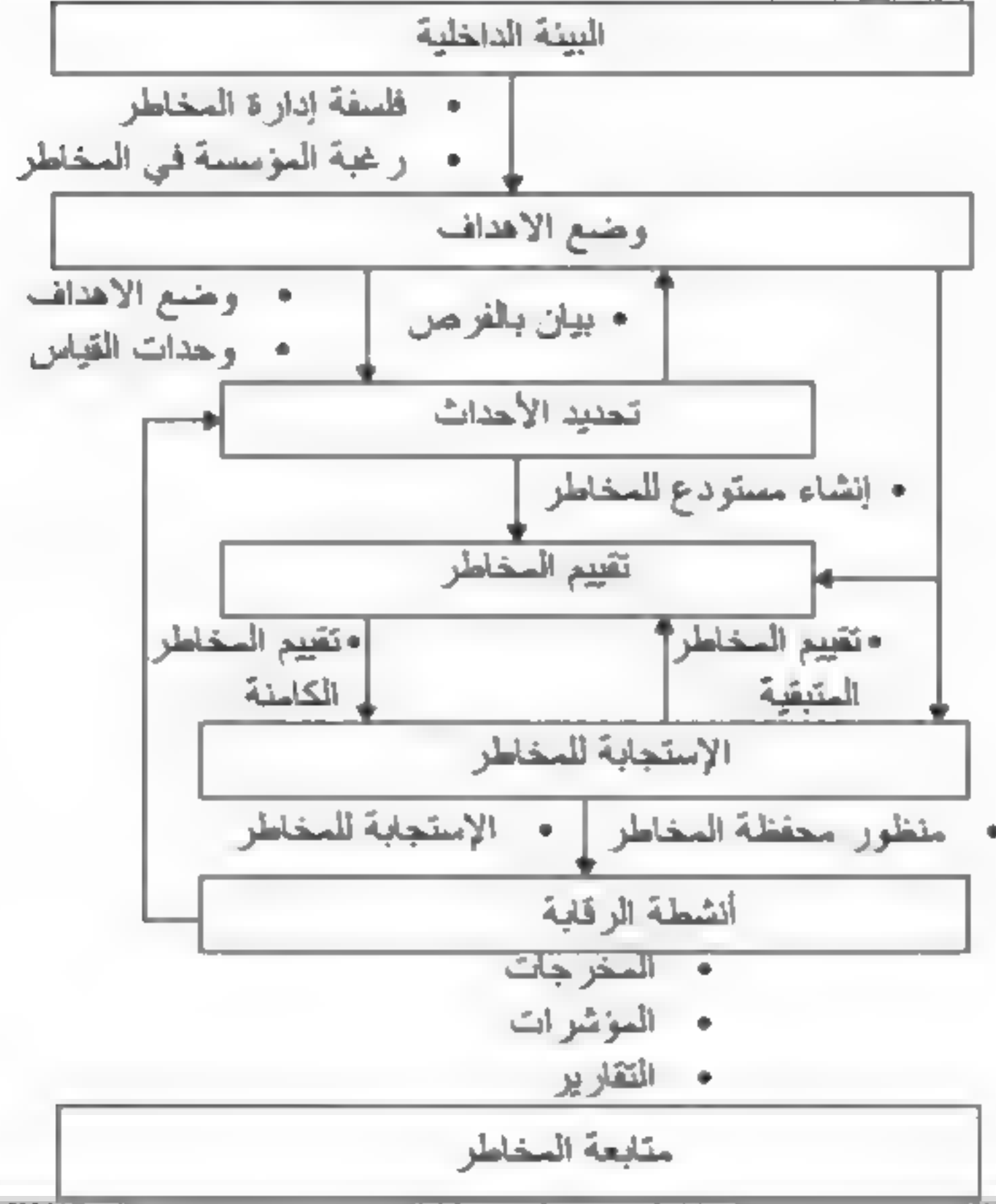
إن هذه الأنشطة الرقابية الخاصة بإطار (COSO ERM) يمكن توسيعها لتشمل مجالات أخرى رئيسية. ويكون بعضها مخصصاً للوحدات المستقلة داخل المؤسسة، إلا أن كل نشاط من هذه الأنشطة، سواء كان بشكل فردي أم جماعي، ينبغي أن يكون من العناصر المهمة في دعم إطار إدارة المخاطر المؤسسية للمؤسسة.

مكونات إطار (COSO ERM): المعلومات والاتصالات:

على الرغم من وصف المكون الخاص بالمعلومات والاتصالات على أنه بند منفصل في الشكل التوضيحي (٨-١) من إطار (COSO ERM)، فإنه يصف مجموعة من الأدوات والعمليات التي تربط بين المكونات الأخرى لإطار (COSO ERM). إن مكون المعلومات والاتصال هذا يربط جميع المكونات الأخرى بعضها مع بعض. ويبين الشكل التوضيحي (٨-٨) تدفقات المعلومات والاتصالات عبر مكونات (COSO ERM) الأخرى. فعلى سبيل المثال، يتلقى مكون استجابة المخاطر مدخلات المخاطر المتبقية والمتأصلة من مكون تقييم المخاطر وكذلك دعم درجة تحمل المخاطر من مكون وضع الأهداف. ثم يقوم مكون استجابة المخاطر الخاص بإدارة المخاطر المؤسسية (ERM) بتقديم استجابة المخاطر وبيانات محفظة المخاطر إلى أنشطة الرقابة، وكذلك التغذية الراجعة لاستجابة المخاطر إلى مكون تقييم المخاطر. وبالنظر إلى مكون المتابعة كونه قائماً بمفرده، نجد أنه لا يوجد به اتصال معلومات مباشر، لكن به مسؤولية شاملة عن مراجعة كل هذه الوظائف.

شكل توضيحي (٨-٨)

تدفق المعلومات والاتصال عبر مكونات ERM



وبينما يكون من السهل نسبياً رسم مثل هذا المخطط البسيط للتدفق لبيان الكيفية التي ينبغي أن تُرسل بها المعلومات من أحد مكونات إطار (COSO ERM) إلى الآخر؛ فإن تلك العملية تكون في كثير من الأحيان أكثر تعقيداً في ربط مختلف مسارات النظم والمعلومات معاً. فلدى العديد من المؤسسات شبكة ويب معقدة من نظم معلومات لا تقوم دائماً على نظم معلومات مرتبطة بشكل جيد لخدمة عملياتها التشغيلية والمالية الأساسية. وتصبح هذه الروابط أكثر تعقيداً عند محاولة ربط عمليات إدارة المخاطر المؤسسية المختلفة نظراً لأن العديد من التطبيقات الأساسية للمؤسسات لا تتلائم بشكل مباشر مع عمليات تحديد المخاطر وتقييم المخاطر واستجابة المخاطر.

ستكون تلك المبادرة الخاصة بإدارة المخاطر المؤسسية قليلة القيمة ما لم يتم إيصال رسالة حول أهمية هذه المبادرة الخاصة بإدارة المخاطر المؤسسية (ERM) إلى جميع أصحاب المصلحة في المؤسسة. ففي كثير من الأحيان ينبغي أن يكون ذلك في شكل رسالة موجهة من الرئيس التنفيذي (CEO)، والفكرة من وراء ذلك هي إيصال رسالة توضح أهمية إدارة المخاطر المؤسسية في جميع أنحاء المؤسسة. وهذه النوعية من الرسائل تكون ذات قيمة عالية، وخاصة عندما ترغب المؤسسة في إيصال رسالة، على سبيل المثال، مفادها أنه على جميع أصحاب المصلحة أن يكونوا حذرين جداً بشأن تبني بعض المشاريع التي قد تنطوي على مخاطر. وتكون العملية أكثر صعوبة إذا كانت المؤسسة تريد أن تفيد بأنه يجب أن نترك بعض العوامل خارج نطاق سيطرتنا قليلاً ويجب علينا تقبل بعض المخاطر أحياناً. إن الرسالة التي يتم تفسيرها بشكل غير صحيح يمكن أن تفتح الباب على مصراعيه بشكل فعال وبشكل غير ملائم للقرارات والمشاريع المحفوفة بالمخاطر.

مكونات إطار (COSO ERM): المتابعة

تم وضع هذا المكون في قاعدة مجموعة المكونات الأفقية للإطار، فالمتابعة في إطار (COSO ERM) ضرورية لتحديد ما إذا كانت جميع عناصر إدارة المخاطر المؤسسية المثبتة لا تزال تعمل على نحو فعال أم لا. ويقوم أفراد المؤسسة بتغيير عمليات الدعم وتنفيذها وكذلك الشروط الداخلية والخارجية المحيطة. ولبناء مستوى معين من الثقة لدى جميع الأعضاء في المؤسسة في أن إدارة المخاطر المؤسسية لديهم تعمل بشكل فعال ودائم، لابد من وضع عنصر المتابعة الخاص بإدارة المخاطر المؤسسية وتفعيله.

إن عمليات المتابعة الجارية يمكن أن تكون وسيلة فعالة للإشارة إلى الاستثناءات أو الانتهاكات التي تحدث في عملية إدارة المخاطر المؤسسية بشكل عام. ولوضع إطار فعال لإدارة المخاطر، لابد من توسيع نطاق هذه المتابعة لتشمل المراجعات الجارية حالياً لجميع العمليات الخاصة بإدارة المخاطر المؤسسية التي تمتد من عملية تحديد أهداف الأنشطة الرقابية الخاصة بإدارة المخاطر المؤسسية الجارية حالياً إلى أن تصل إلى سير عمل تلك الأنشطة والتقدم الحاصل بها. وقد تشمل المتابعة الخاصة بإطار (COSO ERM) الأنشطة التالية:

• تطبيق آلية إدارية قوية ومستمرة لرفع تقارير عن الأوضاع النقدية ومبيعات الوحدة وغيرها من البيانات المالية والتشغيلية الرئيسية. ولا يجب على المؤسسة المنظمة تنظيمياً جيداً أن تنتظر حتى نهاية الشهر المالي أو ما هو أبعد من ذلك لإعداد مثل هذه النوعيات من تقارير الحالة التشغيلية والمالية. وينبغي توسيع نطاق أدوات إعداد التقارير لتشمل مقاييس رئيسية لإدارة المخاطر المؤسسية، متضمناً ذلك بعض أشكال التقارير الخاطفة التي تجري على جميع المستويات المناسبة للمؤسسة.

• يجب وضع عمليات خاصة برفع تقارير دورية لمتابعة الجوانب الرئيسية لمعايير المخاطر المعمول بها، متضمنة أموراً كمعدلات الخطأ المقبولة أو العناصر المرتقبة. فبدلاً من مجرد الإبلاغ عن إحصائيات دورية، ينبغي لمثل هذه التقارير أن تؤكد التنبيهات المتعلقة بالمخاطر مثل الاتجاهات والمقارنات الإحصائية مع الفترات السابقة.

• الإبلاغ عن الوضع الحالي والدوري للنتائج المتعلقة بالمخاطر والتوصيات الواردة في تقارير التدقيق الداخلي والخارجي.

• تحديث المعلومات المتعلقة بالمخاطر باستخدام مصادر كالقوانين الحكومية المنقحة واتجاهات الصناعة والأخبار الاقتصادية العامة. ونؤكد مرة أخرى أنه ينبغي أن يكون هذا النوع من التقارير الاقتصادية والتشغيلية متاحاً للمديرين على جميع المستويات.

وتشير متابعة التقييم المستقل أو الفردي إلى المراجعات التفصيلية لعمليات المخاطر الفردية التي يقوم بها مراجع مؤهل، مثل إدارة التدقيق الداخلي. وقد تقتصر المراجعة هنا على مجالات محددة أو تشمل عملية إدارة المخاطر المؤسسية الكاملة لوحدة تنظيمية. وفي هذا النوع الأخير من المراجعة يمكن الاستعانة بخبراء استشاريين خارجيين مؤهلين لتقييم فاعلية إدارة المخاطر المؤسسية في المؤسسة بأكملها. ومن ناحية أخرى، فبالنسبة للعديد من المؤسسات، قد تكون مؤسسة التدقيق الداخلي القوية هي المصدر الداخلي الأفضل للقيام بتنفيذ مراجعات إدارة المخاطر المؤسسية. وسواء تم ذلك من خلال مدققين داخليين أم مستشارين خارجيين أو كادر من الموظفين المدربين في المؤسسة، فإن أي مراجعة محددة من المراجعات الفردية الخاصة بعمليات إدارة المخاطر المؤسسية قد تستخدم الأدوات التالية:

- **رسم خرائط سير العمليات:** كجزء من أي عملية محددة لإدارة المخاطر المؤسسية، يتعين على الأطراف المسؤولة تطوير مخططات توثق عمليات إدارة المخاطر المؤسسية الخاصة بهم. ويتطلب هذا النظر في الوثائق التي أعدت لهذه العملية لتحديد ما إذا كانت وثائق العملية صحيحة نظراً للظروف الحالية ولإجراء التعديلات الملائمة على مخططات العمليات.
- **مراجعات المخاطر والمواد الرقابية:** إن عملية إدارة المخاطر المؤسسية ينتج غالباً عنها كمية كبيرة من المواد الإرشادية والإجراءات الموثقة وصيغ لتقارير جديدة وما شابه ذلك. وكذلك تكون هناك قيمة حقيقية بالنسبة للفريق المخصص للقيام بمهام إدارة المخاطر المؤسسية أو لفريق التدقيق الداخلي أو لفريق ضمان الجودة الخاص بالمؤسسة عند قيام أي منهم بمراجعة المواد المتعلقة بالمخاطر والمتابعة من ناحية فاعليتها.
- **المقارنة المعيارية:** ويقصد بها هنا عملية النظر في الإدارات الأخرى المعنية بإدارة المخاطر المؤسسية لتقييم عملياتهم التشغيلية وتطوير نهج قائم على أفضل ممارسات الآخرين. إن مهمة جمع هذه المعلومات للمقارنة بها تكون غالباً مهمة صعبة عندما تمتنع في كثير من الأحيان المؤسسات المتنافسة عن تبادل البيانات التنافسية. وتعمل هذه العملية بشكل مثالي عندما يكون هناك اتصالات وعلاقات مهنية محسنة ومباشرة من نوع واحد لواحد، ومعلومات عن الطريقة التي استخدمها البعض لحل بعض المشاكل المماثلة التي تكون غالباً قيمة ومفيدة للغاية.
- **الاستبيانات:** طريقة جيدة لجمع المعلومات من مجموعة واسعة من الناس، ويمكن إرسال الاستبيانات إلى أصحاب المصلحة المعنيين مع طلبات الحصول على معلومات محددة. يعد هذا أسلوب قيم للمتابعة عندما يكون المستهدفون من الاستطلاع منتشرين في أماكن جغرافية مختلفة، مثل مسح متابعة المخاطر للعاملين في مؤسسة تجزئة على الصعيد الوطني.
- **جلسات ميسرة:** يمكن جمع معلومات قيمة غالباً من خلال سؤال أشخاص يتم اختيارهم للمشاركة في جلسة مجموعة التركيز يرأسها قائد مؤتمر ذو مهارة. وهذا هو النهج المتبع من قبل العديد من المؤسسات لجمع معلومات بحوث السوق من خلال ما يسمى بمجموعات التركيز. ويمكن لهذا النهج العام نفسه أن يستخدم لجمع فريق من الناس - في كثير من الأحيان من المناصب المختلفة في المؤسسة - لمراجعة وضع المخاطر المؤسسية لمجال معين.

إن الغرض من عملية المتابعة هذه هو تقييم مدى الجودة التي يعمل بها إطار إدارة المخاطر المؤسسية في المؤسسة. ولابد من إبلاغ المديرين المسؤولين في إدارة المخاطر المؤسسية في منطقة محددة يتم حالياً متابعتها وفي المكتب الخاص بإدارة المخاطر المؤسسية بأوجه القصور الموجودة. إن المفهوم الكامن وراء متابعة إطار (COSO ERM) ليس للعثور على أخطاء أو نواقص فحسب، ولكن لتحديد المجالات التي يمكن تحسينها في إطار إدارة المخاطر المؤسسية.

أبعاد أخرى في إطار (COSO ERM):

كما أوضحنا في بداية هذا الفصل وطبقاً لما تم وصفه في الشكل التوضيحي (٨-١) فإن إطار (COSO ERM) يكون عبارة عن إطار ثلاثي الأبعاد بفئاته الثمانية باعتبارها بعداً واحداً في الأقسام التي تمت مناقشتها حالاً. والبعدان الآخران عبارة عن فئات الأهداف الأربعة له ممثلة بأعمدتها العمودية، وكيانها هو وحداتها الموضحة في البعد الثالث. وعلى الرغم من أن فئات إدارة المخاطر المؤسسية الثمانية التي تم وصفها حالاً مهمة جداً لفهم إطار (COSO ERM) واستخدامه، فإن هذين البعدين الآخرين للإستراتيجيات والوحدات التنظيمية هامان أيضاً. ولفهم المخاطر المحيطة بالأهداف التنظيمية، يجب على المرء تقييم تلك المخاطر من حيث ربما مخاوف الإبلاغ المرتبطة بهذه المخاطر والوحدة التنظيمية المعنية التي تصبح التركيز الرئيسي للمخاطر.

إن إطار (COSO ERM) يلزم استيعابه من خلال كل الأبعاد الثلاثة الخاصة بإطار إدارة المخاطر المؤسسية، كما أن العملية الفعالة لإدارة المخاطر، مهما كانت مصممة بشكل جيد ويتم تشغيلها بصورة جيدة، فهي توفر فقط الضمان المعقول - لكنه ليس المرغوب - الذي تحقق به المؤسسة أهدافها المتعلقة بالمخاطر في إطار الفلسفة الإدارية والرغبة في المخاطرة التي تم وضعها. ومع ذلك، فلا يهم إن كانت إدارة المخاطر المؤسسية قد تم تصميمها وإدارتها بشكل جيد، إذ يمكن أن توجد إخفاقات ناتجة عن أخطاء بشرية أو أحداث مخاطر ناجمة عن أي من أحداث كثيرة غير متوقعة.

"الكتاب الأحمر" لنموذج الحوكمة وإدارة المخاطر والامتثال التابع للمجموعة المفتوحة للامتثال والأخلاقيات (OCEG GRC)، وإدارة المخاطر، وحوكمة تقنية المعلومات:

تعد المجموعة المفتوحة للامتثال والأخلاقيات (OCEG) منظمة غير ربحية يقودها قطاع الصناعة، وهي تعمل على تطوير المعايير وتساعد المؤسسات على تحسين عمليات الحوكمة وإدارة المخاطر والامتثال الخاصة بها. وبدعم كبير من الصناعة التقنية، قامت مجموعة (OCEG) بوضع نموذج قدرة (GRC) ونشره، ويسمى بـ "الكتاب الأحمر" الصادر عن مجموعة (OCEG) مع معايير حوكمة تقنية المعلومات التي أصبحت معترفاً بها بشكل متزايد في العديد من المؤسسات في جميع أنحاء العالم.

ومع التركيز على حوكمة تقنية المعلومات، يستعرض هذا القسم المواد الإرشادية لنموذج القدرة (GRC) الصادر عن مجموعة (OCEG) (الكتاب الأحمر). وبينما يكون العديد من هذه المواد الإرشادية مشابهة جداً لغيرها من المعلومات الإرشادية لنموذج (GRC) وإطار إدارة المخاطر المؤسسية الموجودة هنا وفي الفصول الأخرى، فإننا نستشعر بأن مجموعة (OCEG) سوف يكون لها تأثير كبير في حوكمة تقنية المعلومات وعمليات نموذج (GRC) في السنوات المقبلة.

إن استخدام مجموعة (OCEG) لكلمة "مفتوحة" في اسمها له معنى ما يخص تقنية المعلومات. فالنظام المفتوح يتبادل بانتظام التغذية الراجعة مع بيئته الخارجية ليقوم على نحو مستمر بتحليل تلك التغذية الراجعة، وضبط الأنظمة الداخلية حسب الحاجة لتحقيق أهداف النظام، ومن ثم ينقل المعلومات الضرورية مرة أخرى إلى تلك البيئة. أما النظم المغلقة، على عكس النظم المفتوحة، يكون لديها حدود ثابتة يتم من خلالها تبادل القليل من المعلومات. فالمنظمات التي لديها حدود مغلقة تصبح غالباً راكدة وغير صحية. ومن الأمثلة على الأنظمة المغلقة: البيروقراطية، والاحتكارات، وأنظمة الركود. إن مصطلح "مفتوح" الشائع الاستخدام اليوم في العديد من النظم التقنية الحديثة والمتطورة يعتبر مصطلحاً مناسباً لنموذج القدرة (GRC).

توجد إرشادات نموذج (GRC) الصادر عن مجموعة (OCEG) المفتوحة في وثيقة تسمى الكتاب الأحمر لنموذج القدرة، وتوجد الوثيقة الأساسية على موقع www.oceg.org. ويعود تاريخها إلى شهر إبريل ٢٠٠٩ في وقت نشرنا، وهي متاحة من خلال شبكة الإنترنت، في حين توجد نسخة محسنة متاحة للأعضاء المشتركين. وتتضمن الطبعة الأساسية وصفاً

كاملاً لنموذج (GRC)، لكن النسخة المحسنة ذات التكلفة الإضافية مع القوالب وغيرها من الوسائل المساعدة تكون أيضاً متاحة. ويرتكز نموذج القدرة هذا حول مفهوم يسمى الأداء القائم على مبادئ Principle Performance[®]، وهو نهج نموذج (GRC) المتكامل الذي سوف نناقشه في الأقسام التالية.

كما يوجد لدى نموذج القدرة (GRC) الصادر عن مجموعة (OCEG) العديد من المفاهيم المشابهة تماماً لإطار (COSO ERM) وغيرها من مفاهيم نموذج (GRC) الأخرى التي نوقشت في الفصول الأخرى، وتشمل الأهداف التالية:

- تحسين الأهداف العامة لقطاع الأعمال.

- تحسين ثقافة المنظمة.

- زيادة ثقة أصحاب المصلحة.

- إعداد المؤسسة وحمايتها.

- منع المشاكل والكشف عنها والحد منها.

- الحث على السلوكيات المرغوب فيها وتحفيزها.

- تحسين المسؤولية والكفاءة.

- تحسين القيمة الاقتصادية والاجتماعية.

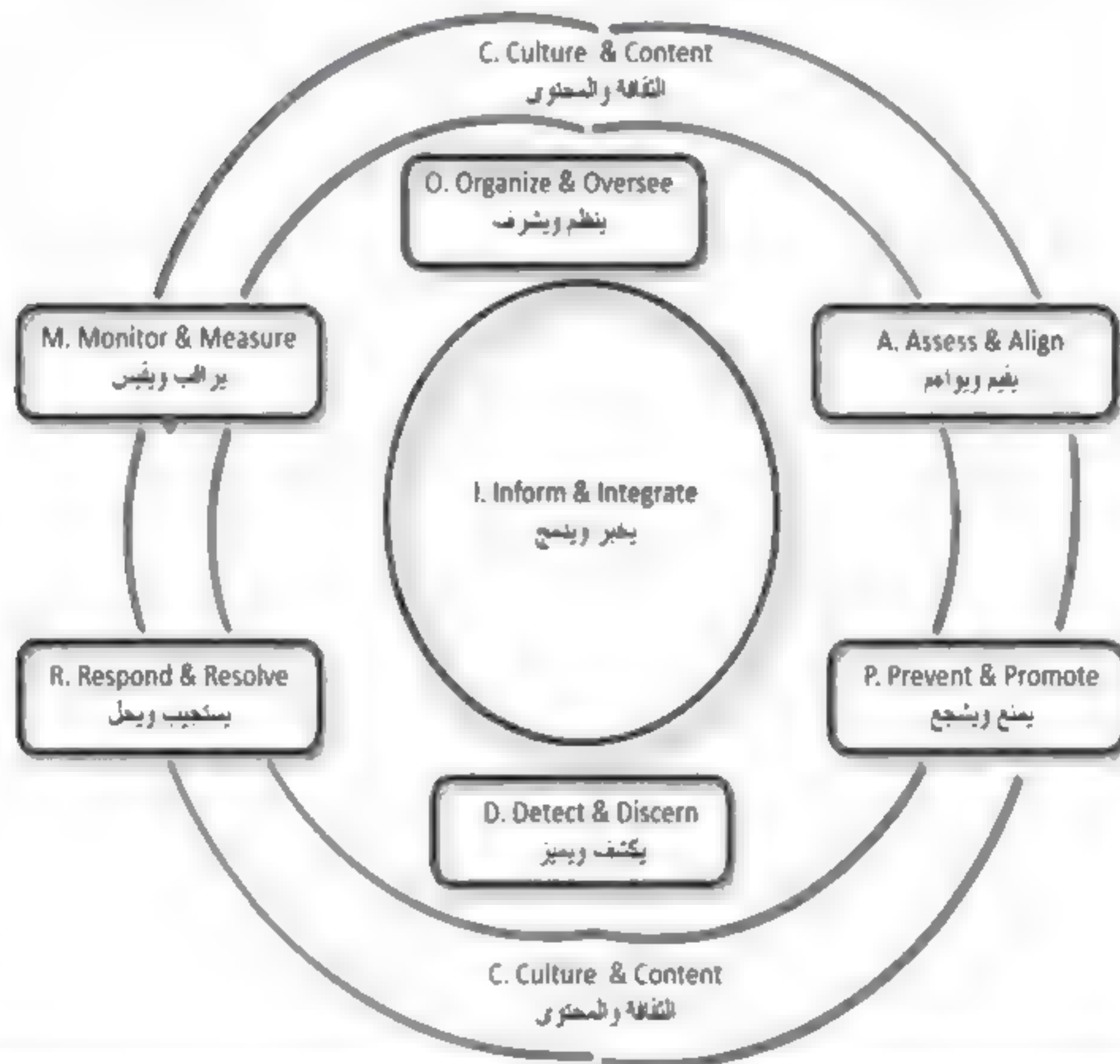
مفهوم الأداء القائم على مبادئ[®] الخاص بمجموعة (OCEG) المفتوحة:

حصلت مجموعة (OCEG) المفتوحة على علامة تجارية لهذا المصطلح وتستخدم هذا المفهوم لوصف الحاجة إلى صياغة الأهداف المالية وغير المالية للمؤسسة لتحقيق جميع الأهداف التي ترغب المؤسسة في تحقيقها أثناء استخدامها لأسلوب فعال وكفاء وقادر على الاستجابة لدعم الحوكمة وإدارة المخاطر والامتثال. إن المفهوم الأساسي هنا هو أن جميع المؤسسات يجب أن تعمل ضمن حدود خارجية وداخلية محددة، فالقوى الخارجية، مثل المتطلبات القانونية والتنظيمية، تضع الحدود الخارجية الإلزامية. ويكون الهدف هو الدمج بين مبادئ وأهداف نموذج (GRC) لمساعدة المؤسسة في أن تعمل على تحسين الأداء بشكل أكثر فاعلية.

ومن أجل أن تحقق المؤسسة مفهوم الأداء القائم على مبادئ، يجب عليها أن تحدد بوضوح رسالتها ورؤيتها وقيمها وتحديد الأهداف التي تسعى إلى تحقيقها. ويجب أن تحدد كيف ستحقق هذه الأهداف في الوقت الذي تقوم به أيضاً بمعالجة المخاطر والأمر الضبابية التي تحتل الشك وحماية ووضع قيمة مضافة وتحديد فرص جديدة ومحاولة البقاء ضمن حدود معينة للسلوك الأخلاقي. ويجب على المؤسسة أن تعمل على جعل هذه الخيارات شفافة لأصحاب المصلحة الداخليين والخارجيين وأن تحاول تحقيق كل هذا باستخدام نهج متكامل لتحقيق أعلى مستوى ممكن من الأداء.

شكل توضيحي (٩-٨)

نموذج القدرة (GRC) الصادر عن مجموعة (OCEG) المفتوحة



ومن أجل تحقيق الأداء القائم على مبادئ لمجموعة (OCEG) المفتوحة، يجب على كل كيان أو وحدة في مؤسسة أن تحدد ما هو "الصواب" بالنسبة لها وبعد ذلك تفعل هذه الأشياء الصحيحة بالطريقة الصحيحة. لقد قمنا باقتباس هذا المفهوم من مواد مجموعة (OCEG) المفتوحة، وهو هدف رفيع المستوى يتجاوز المفاهيم التقليدية لتعزيز قيمة أصحاب المصلحة لتشمل النتائج المرجوة التي تلبي مصالح أصحاب المصلحة لدى المؤسسة واهتماماتهم.

وتعد مفاهيم الأداء القائم على تلك المبادئ من العناصر الرئيسية لنموذج القدرة (GRC) الصادر عن مجموعة (OCEG) المفتوحة كما هو موضح في الشكل التوضيحي (٨-٩). وتصف الأقسام التالية باختصار عناصر هذا النموذج بمزيد من التفصيل، وخاصة عندما يكون لديها أهداف وغايات مختلفة عما كانت عليه في الإطار التقليدي لإطار (COSO ERM) الذي تم وصفه سابقاً في هذا الفصل. ويحدد هذا النموذج مجموعة من المواد والمفاهيم على مستوى عالٍ للغاية، وهي تعد جزءاً من نموذج مجموعة (OCEG) المفتوحة. وتشجيعاً للقارئ المهتم بهذا الأمر، يمكنه الوصول إلى نموذج كامل من خلال عنوان الويب الذي أشرنا إليه سابقاً.

إن كل مدخل من مدخلات النموذج الصادر عن مجموعة (OCEG) المفتوحة يكون مدعوماً من العناصر الرئيسية أو الفرعية الخاصة بنموذج (GRC)، فمثلاً حرف C، مشيراً إلى مكون الثقافة والمحتوى يكون مدعوماً في وثائق مجموعة (OCEG) المفتوحة من خلال أربعة عناصر هي:

C1 سياق الأعمال الخارجية (External Business Context)

C2 سياق الأعمال الداخلية (Internal Business Context)

C3 الثقافة (Culture)

C4 القيم والأهداف (Values and Objectives)

وبعد ذلك يتم تقليل رتبة كل عنصر من عناصر نموذج القدرة (GRC) إلى عناصر فرعية لكل منها. فعلى سبيل المثال، بالنسبة للعنصر C3، الذي يشير إلى الثقافة، يحتوي النموذج على العناصر الفرعية التالية:

C3.1 تحليل الثقافة الأخلاقية (Analyze Ethical Culture)

C3.2 تحليل القيادة الأخلاقية (Analyze Ethical Leadership)

C3.3 تحليل ثقافة المخاطر (Analyze Risk Culture)

C3.4 تحليل إشراك مجلس الإدارة (Analyze Board Involvement)

C3.5 تحليل ثقافة الحوكمة وأسلوب الإدارة (Analyze Governance Culture and Management Style)

C3.6 تحليل مشاركة القوى العاملة (Analyze Workforce Engagement)

وكل عنصر من تلك العناصر يكون مدعوماً أيضاً بعناصر تفصيلية أكثر لزيادة حجم القائمة. وبالإضافة إلى ذلك، فإن النموذج يحتوي على مجموعة من المبادئ وقائمة بمصادر الفشل الشائعة لكل مبدأ من هذه المبادئ، فضلاً عن توجيهات ومراجع لمواد دعم إضافية. ويمكن إيجاد أهداف تفصيلية مماثلة لكل من العناصر والعناصر الفرعية للشكل التوضيحي (٨-١٠). وبالإضافة إلى ذلك، فإن هذا النموذج يحتوي على توثيق الممارسات الفرعية لكل عنصر من العناصر الفرعية. فمثلاً، عنصر (O)، وهو عنصر التنظيم والإشراف، موجود في المركز العلوي يحتوي على عنصر يسمى O2، ويشير إلى الأدوار والمسؤوليات، مع عنصر فرعي O2.4، ويشير إلى تحديد القواعد التشغيلية لنظام (GRC) وتمكينها من العمل. وتوجد توصيفات العناصر والعناصر الفرعية تلك في جميع أنحاء النموذج. فعلى سبيل المثال، يبين الشكل التوضيحي (٨-١٠) أنشطة O2.4.01.

شكل توضيحي (٨-١٠)

مثال على الممارسات الفرعية لنموذج O2.4: GRC تحديد وتمكين القواعد التشغيلية لنظام GRC.

O2.4.01 تحديد الأدوار والمسؤوليات لأنشطة نموذج (GRC) الأساسية التالية:

- المنهجية والسياسة والإجراءات والمعايير والمفردات والصيانة
- تحديد المخاطر والمتطلبات والتحليل والتحسين

- تنفيذ المبادرة / إدارة محفظة المشروعات
- علاقات أصحاب المصلحة
- خط المساعدة أو الخط الساخن
- الاستقصاء والحلول
- قياس الأداء
- الاتصالات متضمنة العلاقات العامة
- إدارة المعلومات
- التقنية

إن هدفنا هنا ليس وصف كل عنصر وعنصر فرعي من هذه العناصر والأنشطة الخاصة بمجموعة (OCEG) المفتوحة بالتفصيل، لكن هدفنا هو وصف المفاهيم العامة وراء نموذج مجموعة (OCEG) المفتوحة. ويمكن للقارئ أن يصل إلى نموذج شامل من خلال موقع ويب www.oceg.org.

بهذا الملخص أو التوضيح للنقاط الفرعية والنقاط المتفرعة منها، يوجد لدينا تفاصيل كافية هنا لمساعدة المؤسسة على إنشاء وتنظيم إدارة للحوكمة وإدارة المخاطر والامتثال (GRC). كما توجد مجموعات جيدة من المبادئ والمصادر المشتركة للإرشادات للمساعدة في تكوين عملية فعالة خاصة بنموذج (GRC) داخل المؤسسة. وقد لخص هذا القسم والأقسام السابقة عناصر نموذج القدرة (OCEG GRC) على مستوى عالٍ للغاية، بعضها مشابه تماماً لعمليات نماذج (GRC) و (COSO ERM) التي تمت مناقشتها في فصول أخرى. في حين يدعو البعض الآخر لاتباع نهج أكثر تفصيلاً وفي بعض الأحيان إلى نهج موجه بدرجة أكبر نحو نظم رقابة إدارية. لكننا مع ذلك نحتفظ بوصف عالي المستوى لا ينصف الدراسة الكاملة التي يمكن العثور عليها في منشور مكون من ٢٤٠ صفحة في شكله الأساسي وبقدر أكبر من التفصيل في وثيقة مطولة. مما يشجع القارئ المهتم إلى القيام بمزيد من البحث في نموذج (OCEG GRC).

مستوى هيئة وضع معايير مجموعة (OCEG) المفتوحة ونطاقها:

ليس لدى مجموعة (OCEG) المفتوحة في الوقت الحاضر هيئة لوضع المعايير الخاصة بحوكمة تقنية المعلومات كما هو موجود مع هيئات (PCAOB) أو (ISO). وبالإضافة إلى ذلك، وعلى الرغم من أنها أصدرت بعض المواد الإرشادية القوية، فإن تلك المعلومات ما تزال مفتقرة إلى مستوى اعتراف كالموجود من خلال المعايير المهنية مثل تلك الصادرة عن معهد المدققين الداخليين (IIA) أو (ISACA). ومع ذلك، فإننا نرى أن أهمية مجموعة (OCEG) المفتوحة وموادها الإرشادية سيزداد في السنوات القادمة وسوف تنمو الاهتمامات والحاجة لعمليات فعالة لنموذج (GRC).

وتكمن إحدى نقاط القوة الرئيسية لمجموعة (OCEG) المفتوحة في أنها منظمة تطوعية تماماً يقوم على إدارتها موظفون جاؤوا على سبيل الإعارة من المنظمات الراعية، وقد شكلوا مجلس قيادة لمجموعة (OCEG) المفتوحة. يشمل الرعاية هنا الشركات المحاسبية العامة الكبرى مثل برايس ووترهاوس كوبرز (PwC) وجرانت ثورنتون (Grant Thornton)، بالإضافة إلى أن هناك العديد من الرعاية من الجهات الرائدة في صناعة تقنية المعلومات الكبرى مثل أوراكل (Oracle) وساب (SAP)، ويأتي في المقام الأول رعاية الصناعة في الولايات المتحدة مثل شركة التأمين الكبرى عون (Aon) ومتاجر التجزئة وول مارت (Walmart). وإذا كان ثمة قلق هنا، فإنه قد يعزى إلى أن مجموعة (OCEG) المفتوحة هي منظمة أمريكية من الأساس وليست منظمة دولية في الحقيقة، لأنها معتمدة على أعضاء المنظمات وأعضاء اللجان الراعية لها. وفي عالمنا المعاصر، إننا بحاجة إلى المزيد من الاهتمام الدولي.

وقد يرغب أحد كبار المديرين المهتمين في استخدام مواد مجموعة (OCEG) المفتوحة هذه على أنها أحد المصادر المرجعية الإضافية، إذ إنها مجموعة واسعة من المواد التي يمكننا فقط توقع زيادة أهميتها في السنوات المقبلة.

ملاحظات:

١. "Tsunami Pacts and Information," Australian Government, Bureau of Meteorology. www.bom.gov.au/tsunami/info/index.shtml
٢. Robert R. Moeller, COSO Enterprise Risk Management: Establishing Effective Governance. Risk, and Compliance Processes. 2nd ed. (Hoboken. NJ: John Wiley & Sons, 2011).
٣. Christine Hauser, "Boeing Board Ousts Chief. Citing Relationship with Executive," New York Times, December 7, 2005.
٤. Enterprise Risk Management-Integrated Framework: Application Techniques (COSO, April 2004).
٥. Scott Patterson. "Breakdown: A Glimpse Inside the 'Plash Crash,'" Wall Street Journal. June 10, 2012. wsj.com/article/SB10001424052702303296604577454330066039896.html?mg=reno64-wsj
٦. اثنين من الباعة اللذين يقومان بتوريد لوحات المعلومات هما موردي البرمجيات بيزنس أوبجيكتس Business Objects وكوجنوس COGNOS.
٧. لمزيد من المعلومات حول مراجعات الرقابة الداخلية الواردة بالبند ٤٠٤. انظر Robert Moeller. Sarbanes-Oxley Internal Controls: Effective Auditing " (with ASS. CobiT, and ITIL (Hoboken. NJ: John Wiley & Sons, 2008).

الجزء الثالث

أدوات وتقنيات إدارة البنية التحتية لحوكمة تقنية المعلومات

الفصل التاسع

حوسبة سحابية وافتراضية وحوسبة محمولة متنقلة

عالم نظم تقنية المعلومات مليء دائماً بالمفاهيم والتقنيات الجديدة المتطورة باستمرار. فبعضها يعد من المفاهيم والتحولات الخاصة بتقنية المعلومات والتي سرعان ما أصبحت ممارسات شائعة ومقبولة. ويمكن اعتبار لغة برمجة الإنترنت الجافا أحد الأمثلة على تلك التقنية الحديثة. فقد أصبحت التطبيقات التي تستخدم الجافا بمثابة الوسيلة التي تسمح بالاتصال بين مواقع الإنترنت المركزية والأنظمة الفردية، كما أصبحت الجافا معياراً لتطوير الإنترنت (شبكة المعلومات العالمية). من ناحية أخرى، فإنه فضلاً عن أن هناك العديد من التقنيات الحديثة التي لاقت في بداياتها المزيد من الاستحسان والدعم والدعاية والترويج في العديد من المطبوعات المتنوعة الخاصة بتقنية المعلومات؛ فإنها لم تحتل مكانة عالية في السوق وسرعان ما تم نسيانها. وفي النهاية، فإن هذه التقنيات "لم تكن تلك الصفقة الكبيرة"، وذلك عندما تم تجاهلها وإهمالها من قبل مستخدمي تقنية المعلومات والسوق التقني أو أن المنافسين قد جاؤوا بعروض أفضل.

لقد كان لدينا بعض التقنيات الحديثة منذ مدة طويلة، وفي الواقع تعد هذه التقنيات حديثة فقط عندما تُقارن بالنظم والعمليات التقليدية لتقنية المعلومات. وقد أسهمت هذه التقنيات في تغيير الطريقة التي نفكر بها في بناء وإدارة نظم تقنية المعلومات والعمليات الداعمة لها. وسوف يقوم هذا الفصل بتسليط الضوء على ثلاث من هذه التقنيات الحديثة التي أصبحت شائعة بشكل متزايد في عمليات تشغيل تقنية المعلومات في الوقت الراهن، فيما ستطرح أيضاً كل تقنية من هذه التقنيات بعض القضايا الخاصة بحوكمة تقنية المعلومات.

في البداية سنتحدث عما أصبح يعرف بالحوسبة السحابية Cloud Computing، وهو المفهوم المرتبط باستخدامنا للإنترنت وشبكة الويب العالمية منذ أواخر التسعينيات من القرن الماضي. يستخدم المهنيون هذه الأيام إحدى أدوات البحث عبر الإنترنت كجوجل مثلاً للبحث عن إجابات لأسئلة أو لجمع المزيد من المعلومات عن موضوع ما. وبينما ينتج

وبشكل فوري عن أحد طلبات البحث التقليدية مدى واسع من "ضربات" أو نتائج البحث لهذا الطلب، فإننا في الواقع لا نفكر كثيراً بالطريقة التي من خلالها استطعنا الحصول على كل تلك النتائج الهائلة وبتلك السرعة الهائلة. فجميع هذه النتائج تأتي من شبكة الإنترنت، سواء كانت من بلادنا أو من العالم الخارجي. ونظراً لأننا لا نستطيع الإشارة إلى نظام أو مصدر محدد على أنه هو المزود للمعلومات الخاصة باستعلامنا عبر شبكة الإنترنت، فإننا نتصور أن تلك المصادر الخاصة بالإنترنت كما لو كانت عبارة عن شبكة اتصالات مترابطة وواسعة، تكون غالباً "سحابة" من المصادر.

تتجاوز مصادر تقنية المعلومات، مجرد كونها محركات للبحث، والتي يتم عرضها بشكل متزايد من خلال سحابة الإنترنت تلك. وسواء كانت تلك السحابة عبارة عن مرفق خدمي محلي أو عالمي أو حتى كانت عبارة عن مركز لإحدى المؤسسات الكبيرة، فنحن نستخدم الحوسبة السحابية بشكل متزايد لبناء وإدارة نظم تقنية المعلومات الخاصة بنا. وسيناقش هذا الفصل بعض القضايا الخاصة بحوكمة تقنية المعلومات والتي تُثار عندما نستخدم تلك السحابة لنظم وعمليات تقنية المعلومات.

ستكون الافتراضية virtualization وقضايا حوكمة تقنية المعلومات الخاصة بها هي التقنية الثانية التي سيتم مناقشتها في هذا الفصل. فعلى الرغم من أن لها أصولاً تعود إلى النماذج السابقة الخاصة بنظم الحاسبات المركزية التي تم إنتاجها من قبل شركة آي بي إم IBM منذ سنوات عديدة، فإن الافتراضية هي المفهوم الذي كان مجهولاً بالنسبة لمعظم المهنيين العاملين في مجال تقنية المعلومات حتى فترة زمنية ليست بالبعيدة. فهي تعود للوقت الذي انتقلنا فيه للمرة الأولى من نظام تقنية معلومات يعتمد على حاسب مركزي واحد إلى العديد من نظم الخادم المتصلة في تقنية المعلومات والتي احتوت في البداية على عدد قليل من هذه النظم ثم زادت بعد ذلك. في البداية كانت عملية توصيل كل نظام خادم بمجموعة من وحدات التخزين والمرفقات الأخرى تعتبر من العمليات السهلة، إلا أن النظم أصبحت أكثر تعقيداً مع نمو إعدادات نظم تقنية المعلومات. هذا بالإضافة إلى أن إدارة عمليات التشغيل الخاصة بتقنية المعلومات قد أدركت مبكراً أن إعداداتها الخاصة بالموارد المتصلة والملحقة بالخادم لم تكن متوازنة بشكل جيد. فعلى سبيل المثال، قد يكون للخادم (أ) إمكانيات كبيرة للذاكرة المؤقتة أو وحدات التخزين الملحقة ولكنه

ربما لا يستخدم كل هذه الموارد على أنها جزء من عمليات التشغيل المجدولة أو الاعتيادية التي تتم على هذا الخادم (أ). في حين قد يكون هناك خادم آخر (ب) به قصور في الموارد ويحتاج إلى بعض الموارد الزائدة عن حاجة الخادم (أ) لتساعده خلال فترة أحمال الحوسبة المرتفعة.

خلال الأيام الأولى للحوسبة الخاصة بنظم "عميل - خادم"، كان يتم ربط تلك الموارد بكل خادم على حدة إما من خلال تعليمات برمجية محددة أو حتى من خلال توصيلات كوابل مادية. ومن ثم فإن عمل تغييرات كنقل بعض الموارد غير المستخدمة من الخادم (أ) إلى الخادم (ب) ليساعده في إنجاز مهامه كانت تستهلك وقتاً طويلاً وفي بعض الأحيان كانت مهمة معقدة. وقد تم حل تلك المشكلة الخاصة باتصال الخوادم بموارد تقنية المعلومات وتحقيق ما يعرف بتوازن الأحمال بين الخوادم عن طريق بعض بائعي نظم إدارة التخزين ابتداءً من العام ٢٠٠٠ تقريباً بواسطة ما يعرف الآن بالنظم الافتراضية.

ففي البيئة الافتراضية، لا تتصل موارد النظام ببعضها البعض بشكل حقيقي أو مادي ولكنها ترتبط بشكل منطقي بواسطة أدوات برمجية خاصة. وبناءً على الطلب على موارد النظم، فإنه يمكن للنظم المنفصلة أن تتصل بشكل افتراضي مع موارد أخرى، بشكل آلي أو تلقائي، بدلاً من استخدام الكوابل المادية اليدوية أو الروابط البرمجية التي كانت تستخدم في السابق. حيث تستطيع البيئة الافتراضية تقديم قدرات كبيرة للإعدادات الضخمة لتقنية المعلومات. من ناحية أخرى، إذا كانت عمليات النظم الافتراضية غير مفهومة أو مطبقة أو مدارة بالشكل المناسب، فإنها قد تثير بعض القضايا المتعلقة بحوكمة تقنية المعلومات. سيقدم هذا الفصل المفاهيم الخاصة بالبيئة الافتراضية لتقنية المعلومات كما يناقش بعض القضايا الرئيسية للحوكمة ذات الصلة بهذا الموضوع.

وسيختتم هذا الفصل بالحديث عن قضايا حوكمة تقنية المعلومات المتعلقة بأجهزة الحوسبة المحمولة الشخصية الواسعة الانتشار والتي لا تستخدم فقط للأغراض الشخصية وإنما تستخدم أيضاً على أنها مكونات لنظم تقنية المعلومات المؤسسية. تعتبر أجهزة الحواسيب اللوحية الصغيرة أو الهواتف الذكية بمثابة أدوات رائعة للاتصالات والوصول إلى الإنترنت والتقاط الصور الفوتوغرافية والعديد من المهام الأخرى. فعلى الرغم من

إطلاقها على أنها أجهزة شخصية، فإنها تسببت في نجاحات كبرى في أماكن العمل. وسيُختم هذا الفصل بمناقشة قضايا حوكمة تقنية المعلومات المتعلقة باستخدام أجهزة الحاسبات الشخصية في بيئة العمل.

التعرف على الحوسبة السحابية:

كان لدى مديري الأعمال القدامى، الذين نشؤوا في عصر الورق والقلم الرصاص، ولسنوات، اعتقاد بأن بعض أعضاء فرق نظم وتطوير تقنية المعلومات العاملين لديهم لهم "مديرون في السُحْب"، في حين أن ما يعرف بالحوسبة السحابية يعد من المفاهيم الحديثة والمتطورة والمهمة بالنسبة للعديد من عمليات تشغيل تقنية المعلومات. وهو وثيق الصلة بالمفاهيم الخاصة بالبنية الموجهة نحو الخدمات (Service-Oriented Architecture) SOA والتي نوقشت في الفصل الثالث عشر من هذا الكتاب، لقد أسهمت الحوسبة السحابية في تغيير الأسلوب المتبع من قبل العديد من المؤسسات في بناء واستخدام تطبيقات تقنية المعلومات.

يُستخدم مصطلح السحابة غالباً هنا وفي العديد من المراجع المنشورة على أنه تعبير مجازي للدلالة على الإنترنت. إن الفكرة التي تكمن خلف سحابة الإنترنت تلك هي أن المستخدمين ليسوا بحاجة إلى (معرفة ب أو خبرة عن، أو سيطرة على) البنية التحتية للتقنية "في السُحْب" التي تدعم التطبيقات القائمة على الإنترنت. وقد تم استحداث هذا المصطلح في مجال صناعة الهواتف، حيث ظل قائماً حتى تسعينيات القرن الماضي، فالبيانات وحتى الدوائر البدائية لشبكة الإنترنت بين الأماكن قد تم ربطها من خلال الأسلاك. ثم بدأت بعد ذلك شركات الهواتف البعيدة المدى بتقديم خدمات الشبكة المحلية الافتراضية اللاسلكية لنقل البيانات. وقد أسهم نمو تلك الشبكات اللاسلكية والإنترنت وشبكة الويب العالمية في تطوير الطريقة التي نفكر فيها بخدمات تقنية المعلومات هذه الأيام.

إن الحوسبة السحابية، على كل حال، تعد أكثر من مجرد شبكة إنترنت، فهي الطريقة التي نستخدمها نحن للتفكير بالخدمات التي تقدمها التطبيقات التي تسكن شبكة الإنترنت. ولأنه من المستحيل أن يكون هناك تحديد مسبق لمسارات حركة الإنترنت بشكل دقيق، فقد تم استخدام مصطلح السحابة ليدل مجازاً على المرافق الخاصة بخدمات تقنية المعلومات والتي تعد أحد مسؤوليات مقدمي الخدمات، إضافة إلى البنية التحتية للشبكة.

وسرعان ما تبع ذلك كل من مفاهيم المنتجات البرمجية أو الخدمات عبر الإنترنت أو مفهوم البنية الموجهة نحو الخدمات SOA.

يقوم بائعو البرمجيات عادة بعرض المنتجات البرمجية الخاصة بهم على شكل خدمات على الإنترنت بدلاً من أن تكون على شكل تطبيقات تسكن خوادم العملاء الشخصية. وخير مثال هنا - أحد رواد مثل هذا النوع من المنتجات - هو مورد البرمجيات الخاصة بإدارة علاقات العملاء سيلزفورس (www.salesforce.com/crm/products.jsp) (SalesForce). فهذا المورد للأدوات البرمجية الخاصة بتتبع العملاء والمبيعات لا يقوم ببيع منتجاته كمجموعة من البرامج المحملة على الأقراص المدمجة CDs ليقوم العميل باستخدامها. لكنه يقوم بعرض جميع البرامج والوثائق الخاصة بشركة Salesforce على شبكة الإنترنت، حيث يقوم العملاء بدفع المال مقابل المنتجات البرمجية فقط عندما يستخدمونها. حيث تُستخدم تطبيقات شركة Salesforce على شكل خدمات مقدمة للعملاء.

يوضح الشكل التوضيحي (٩-١) هذا المفهوم الخاص بالحوسبة السحابية. وقد قمنا بتسليط الضوء على مقدمي الخدمات الذين يقومون بعرض منتجات خاصة بالحوسبة السحابية هذه الأيام مثل شركة أمازون Amazon وشركة جوجل Google وشركة مايكروسوفت Microsoft وشركة سيلز فورس Salesforce كذلك. وما هذه إلا عينة بسيطة عن بعض التطبيقات الحالية، وبالتأكيد هناك ما هو أكثر بكثير. وفيما يلي بعض فوائد التطبيقات التي تعمل في بيئة الحوسبة السحابية:

- **خفض تكاليف البنية التحتية نتيجة المركزية:** مع وجود تطبيقات تقنية المعلومات على البيئة السحابية، لم يعد هناك حاجة للحفاظ على المستوى نفسه من العمليات الخاصة بإدارة التغيرات البرمجية وغيرها من الضوابط المتعلقة بتلك التطبيقات الموجودة في البيئة السحابية. قد يكون لهذا الأمر إلى حد ما جانب إيجابي وآخر سلبي بالنسبة للبعض نظراً لأنك تحصل فقط على السمات والأشكال التي يسمح بها التطبيق.

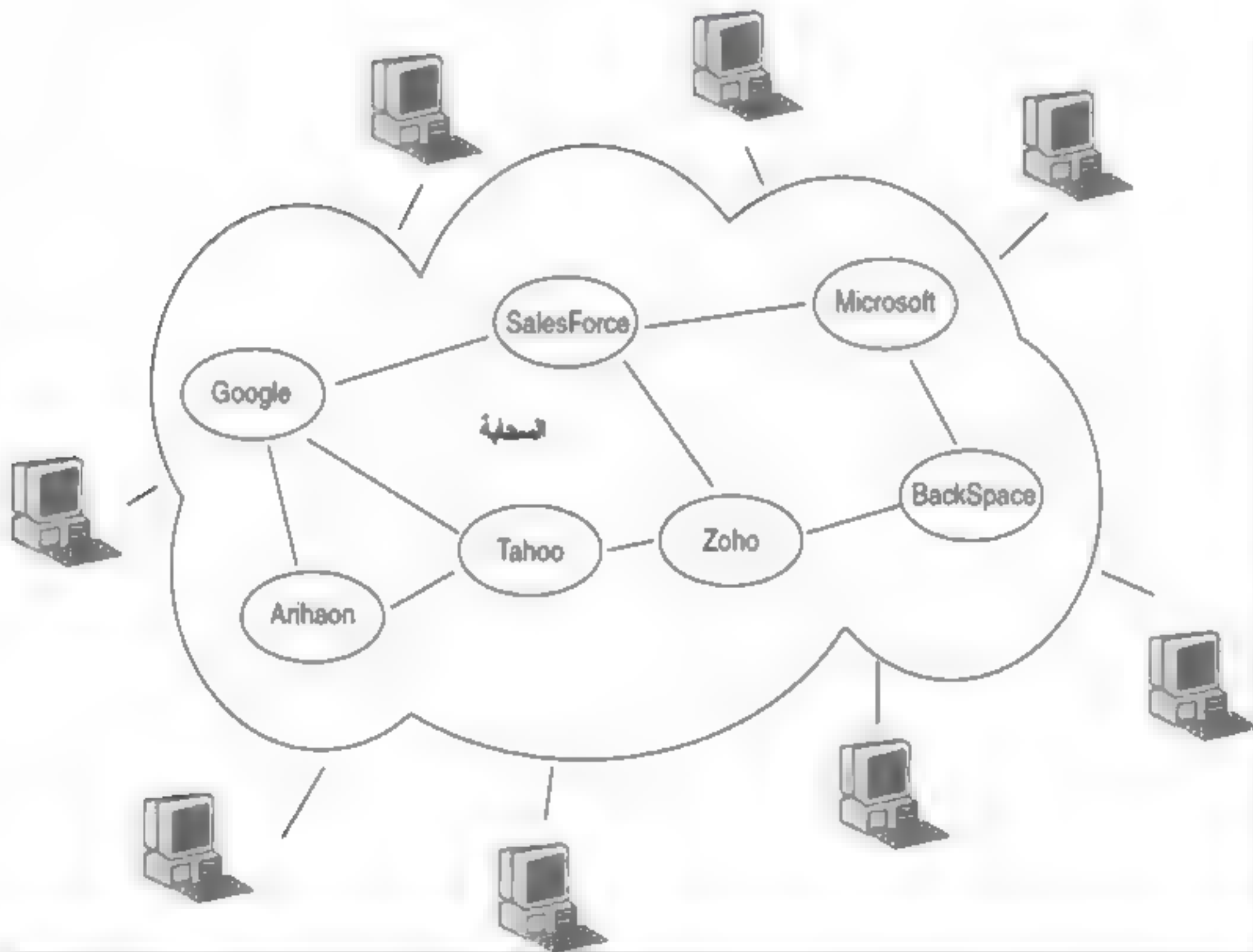
- **ارتفاع سقف ساعات الأحمال:** يمتلك مقدمو الخدمات السحابية كشركة أمازون أو جوجل مزارع خوادم ضخمة جداً لنظم تقنية المعلومات وبقدرات تخزينية هائلة، حيث تبدو ساعات الأحمال التشغيلية لحواسيبهم وكأنها تقريباً لا محدودة.

- متابعة الأداء المناسب للنظم من قبل مقدم الخدمة: يستطيع مقدمو الخدمات السحابية أن يقوموا بمراقبة جميع خدمات تقنية المعلومات المقدمة من مزود البيئة السحابية وكذلك مراقبة المستخدمين المهمين. ونتيجة لذلك يجب أن يكون لدى مقدم الخدمة أدوات رقابية معمول بها لتقديم تغييرات التحسين الخاصة بالعملية بالشكل المطلوب.

- مرونة التطبيقات وخدمات تقنية المعلومات: لقد قام مقدمي خدمات البيئة السحابية بعمل نسخ طبق الأصل للحلول -وهو ما يعرف باسم (المرآوية) mirroring - التي يمكن أن تستخدم في حالات الكوارث أو في توازن الأحمال عند ازدحام البيانات. فسواء كانت هناك كارثة طبيعية تستلزم الحاجة لموقع آخر في منطقة جغرافية مختلفة، أو كان هناك ازدحام شديد للبيانات، إذ يكون مقدمو خدمات البيئة السحابية عادة على استعداد لتقديم الحلول المناسبة.

شكل توضيحي (٩-١)

مفاهيم الحوسبة السحابية



إن مديري الشركات الذين يقومون بتطبيق حوكمة تقنية المعلومات بحاجة إلى اتباع نهج مختلف في مراجعة الضوابط الداخلية المتعلقة بتطبيقات البنية الموجهة نحو الخدمات SOA بالإضافة إلى فهم الأمور الخاصة بأمن تقنية المعلومات في بيئة الحوسبة السحابية. لقد أصبحت خدمات شبكة الويب وغيرها من خدمات البنية التحتية تُقدّم وبشكل متزايد في البيئة السحابية، الأمر الذي يستدعي إعادة التفكير ببعض الاعتبارات الخاصة بعمليات التدقيق والرقابة.

مراجعة الضوابط الخاصة بتطبيقات الحوسبة السحابية:

كون التطبيق يعمل انطلاقاً من بيئة البنية الموجهة نحو الخدمات SOA - فهذا لا يعني أبداً أن الحاجة إلى تقييم وفهم الضوابط الداخلية الخاصة بهذا التطبيق لم تعد موجودة. بل يجب أن يستمر التطبيق القائم على البنية الموجهة نحو الخدمات في مسارات التدقيق وإجراءات فحص الأخطاء نفسها وغيرها من الممارسات الجيدة التي يمكن أن نجدها في أي تطبيق تقنية معلومات محكم الرقابة. في الغالب يمكننا توقع أن تطبيق الأعمال الذي يعمل تحت رعاية إحدى الشركات الكبرى التي تقدم الخدمات السحابية مثل جوجل، الذي يُستخدم غالباً من قبل عدد كبير من العملاء في جميع أنحاء العالم، لديه ضوابط داخلية ملائمة.

تمثل الحوسبة السحابية تغييراً جوهرياً في الطريقة التي تعمل وتدار بها التطبيقات، وبينما لا يوجد سوى عدد محدود من الباعة الذين يقومون اليوم بتقديم التطبيقات البرمجية القائمة على الخدمات، فإن هذا الرقم من مقدمي الخدمة مرشح للزيادة. هناك مستوى ضمني من الثقة في تلك الخدمات المقدمة من قبل العديد من مزودي الخدمة تحت مظلة سحب الإنترنت تلك، إلا أن قادة إدارة الأعمال وتقنية المعلومات لتلك الخدمات إلى جانب مدققي تقنية المعلومات يجب أن يحصلوا على ضمانات بأن هذه التطبيقات القائمة على السحابة تتم مراقبتها بشكل جيد. كما يجب على جميع المستخدمين المباشرين وغير المباشرين للحوسبة السحابية تطوير مستوى قوي من الثقة في الخدمات البرمجية والبنية التحتية التي تشكل السحابة الخاصة بالمؤسسة. يجب أن يلتقي المسئول التنفيذي، الذي يحدد ما إذا كان قسم تقنية المعلومات لديه سيقوم بتبني إستراتيجية الحوسبة

السحابية فيما يخص بعض تطبيقاته في المؤسسة، مع إدارة تقنية المعلومات لفهم مثل هذه المبادرات. وفيما يلي بعض القضايا الأساسية فيما يخص حوكمة وضمان تقنية المعلومات في الحوسبة السحابية:

- **الشفافية Transparency:** يجب على مقدمي الخدمات السحابية أن يكونوا قادرين على إثبات وجود ضوابط أمنية فعالة وقوية، تضمن للعملاء بأن معلوماتهم مؤمنة على نحو جيد ضد أي عملية وصول غير مصرح بها، أو تغيير، أو تخريب. فالأسئلة الرئيسية التي توجه لأي مقدم خدمات يعرض التطبيقات السحابية هي:

- ما نوعية الموظفين العاملين لدى مقدمي خدمات البيئة السحابية الذين يستطيعون الوصول لمعلومات أي عميل؟

- هل يتم الحفاظ على الفصل بين مهام موظفي مقدمي الخدمات السحابية؟

- كيف يتم الفصل بين الملفات والبيانات الخاصة بالمعلومات المختلفة للعملاء؟

- ما الضوابط الموضوعة لمنع أي خروقات أمنية ورقابية في السحابة والكشف عنها والرد عليها؟

- **الخصوصية Privacy:** يجب على مقدمي خدمات الحوسبة السحابية إعطاء ضمانات بأن ضوابط الخصوصية المستخدمة ستمنع الخروقات الأمنية وتكشف عنها وترد عليها في الوقت المناسب، وبأن لديها خطوط اتصالات قوية ويتم فحصها بشكل دوري.

- **الامتثال Compliance:** لكي يتم الامتثال لمختلف القوانين واللوائح والمعايير المعمول بها، فقد تكون هناك مخاوف متعلقة بالحوسبة السحابية من حيث أن البيانات قد لا تُحفظ في مكان واحد بل ربما لا يكون من السهل استرجاعها. فمن المهم جداً ضمان أنه عند طلب البيانات من قبل أصحابها، فإنه يمكن تقديمها دون المساس بالبيانات الأخرى. عند استخدام الخدمات السحابية، يجب أن تكون هناك ضمانات بأن المؤسسة تستطيع الحصول على بياناتها عندما تحتاجها، أو أن الجهة المقدمة للخدمة قد تطالب بحقوقها في حجب البيانات عن السلطات.

- **تدفق البيانات عبر الحدود:** مع وجود احتمالية تخزين المعلومات السحابية في أي مكان داخل السحابة، فقد يكون معرفة الموقع الجغرافي للمعلومات من إحدى القضايا أو

المشاكل. فالموقع الجغرافي للبيانات هو الذي يفرض الالتزام القانوني والقضائي للفصل في الدعاوى. ولا يزال هناك العديد من المسائل القانونية التي لم تحل بعد في هذا المجال.

- **الاعتماد:** يجب أن يزود مقدمو خدمات الحوسبة السحابية عملاءهم بالضمانات الكافية على أنهم يقومون بعمل الأشياء "الصحيحة". لذلك، يجب أن نرى في المستقبل عمليات تدقيق مستقلة يقوم بها طرف ثالث و/أو تقارير عن الخدمة لأحد المدققين والتي ستصبح جزءاً حيوياً لأي برنامج ضمان يخص مقدم خدمات الحوسبة السحابية. وستتبع هذه التقارير المعيار الصادر عن المعهد الأمريكي للمحاسبين القانونيين AICPA والمعروف باسم معيار التدقيق رقم ٧٠^(١) (SAS 70) الذي سيصبح أكثر أهمية في السنوات القادمة.

إن وجود المعايير القوية والفعالة من شأنه أن يساعد المؤسسات على كسب المزيد من الضمانات المتعلقة بالضوابط الداخلية وقضايا أمن تقنية المعلومات الخاصة بمقدمي خدمات الحوسبة السحابية. على كل حال فإنه حتى وقت نشر هذا الكتاب لم يكن هناك معايير محددة ومتاحة بشكل علني فيما يتعلق بالحوسبة السحابية.

وفي ظل عدم وجود مجموعة محددة أو معرفة لمثل تلك المعايير، فإنه يجب على المدير الأول أو مدقق تقنية المعلومات الذي يقوم بمراجعة التطبيقات المقدمة من قبل مزود خدمات الحوسبة السحابية أن يطلب من مزود الخدمة تقديم ضمانات كافية في ثلاث مجالات رئيسية على الأقل هي:

١- **الأحداث Events:** يجب أن يقوم مزود الخدمة وبشكل منتظم بتوثيق جميع التغيرات، والإبلاغ عنها وعن غيرها من العوامل الأخرى التي تؤثر في إتاحة نظام البنية الموجهة نحو الخدمات SOA.

٢- **سجلات Logs:** يجب أن يقوم مزود الخدمة بتقديم معلومات شاملة عن تطبيق البنية الموجهة نحو الخدمات SOA الخاص بالمؤسسة وعن بيئة التشغيل الخاصة به.

٣- **المراقبة Monitoring:** أي عملية رقابية من هذا النوع لا يجب أن تكون تطفلية ويجب أن تكون مقتصرة فقط على الاحتياجات المنطقية الخاصة بمقدم الخدمة السحابية لكي يقوم بتشغيل مرافقه.

تتيح الحوسبة السحابية بعضاً من الفرص الجديدة والهامة من أجل إعادة النظر فيما يتعلق بأمن وضوابط تقنية المعلومات من أجل غد أفضل، ولا بد أن يتبع ذلك قريباً معايير ذات طابع أكثر رسمية في ما يخص الحوسبة السحابية. ونستطيع أن نتوقع مشاهدة ما هو أكثر من ذلك بكثير في المستقبل نظراً لأن التطبيقات السحابية والحوسبة السحابية لمزودي الخدمات في نمو ونضوج مستمر.

تحديات الأمن والخصوصية في بيئة الحوسبة السحابية:

إن استخدام التطبيقات التي تعمل في بيئة الحوسبة السحابية قد عمل على نقل مجموعة كبيرة من التحديات والمسؤوليات من إدارة تقنية المعلومات الخاصة بالمؤسسة بشكل أساسي إلى البيئة التي قد فرضت فيها بعض المسؤوليات من قبل مقدم خدمة الحوسبة السحابية، في حين لا يزال البعض الآخر منها من مهام إدارة تقنية المعلومات الخاصة بالمؤسسة. وهذا هو التحدي بالنسبة لإدارة تقنية المعلومات والمدققين الداخليين التابعين لها على حد سواء، والذين يجب عليهم فهم ومعرفة مكونات أمن المعلومات والخصوصية التي تخص مقدمي خدمات الحوسبة السحابية الذين اختاروهم بأنفسهم.

لا تزال الحوسبة السحابية عبارة عن توجه جديد ومتطور. فعلى الرغم من العدد المتزايد لمزودي الخدمات الذين يقومون بتقديم خدمات استضافة التطبيقات السحابية، وعلى الرغم أيضاً من وجود مزودي خدمات مثل شركة جوجل وشركة أمازون الذين يقومون ببناء بيئات ضخمة ومعقدة ومتعددة الخوادم للحوسبة السحابية، إلا أنه لا يوجد هناك مجموعة محددة لأفضل الممارسات المتفق عليها بين مختلف هؤلاء المزودين للخدمات السحابية. في بعض الأحيان نرى أن هذا التوجه الموجود اليوم لدى المؤسسات لتحويل بعض موارد تقنية المعلومات الخاصة بها إلى مقدمي خدمات الحوسبة السحابية، ولو بطريقة ربما تكون غريبة بعض الشيء، يشبه في بعض عناصره عملية الانتقال إلى ما كان يعرف باسم مكاتب خدمات تقنية المعلومات والتي ظهرت في أوائل الثمانينيات من القرن الماضي والتي أصبحت الآن من مفاهيم الماضي.

قررت العديد من المؤسسات في منتصف وحتى نهاية سبعينيات القرن الماضي أنها بحاجة إلى الانتقال من عمليات وحدة سجلات البطاقات المثقبة إلى أحد نظم الحواسيب

المركزية mainframe المتطورة. لذا فقد تم إضافة الكثير من الكوادر البرمجية المطوّرة للنظم والنظم الحاسوبية المركزية الجديدة التي تم بناؤها وتنفيذها، غير أن النتائج كانت مخيبة جداً للآمال. حيث كانت المشكلة المتكررة هنا هي أن نظم الحوسبة المركزية الجديدة تلك لا تملك السعة الكافية لمعالجة الكميات المطلوبة من بيانات المؤسسات، وفي حال قامت بذلك، كانت تواجه العديد من مشاكل الصيانة والتوقف عن العمل.

وقد كان الحل بالنسبة للعديد من المؤسسات وقتها هو تحويل ونقل عمليات التشغيل الخاصة بنظمهم الحاسوبية إلى ما كان يعرف وقتها بمكاتب الخدمة - وهو أحد أكبر موارد نظم الحاسب المركزية الذي كان يقوم بتجميع المدخلات للعديد من العملاء ومعالجة النظم الخاصة بهم وتسليم تقارير بالمخرجات. ولم تكن مكاتب خدمات النظم الحاسوبية تلك تعمل على نحو جيد أو مناسب بالنسبة للجميع. فقد كان العديد من المشاركين في تلك الخدمات يتم دون إدراك ووعي تام لما سيحصلون عليه من حيث الخدمات وإمكانية المحافظة على أمن وسلامة معلوماتهم وإمكانية متابعة الضوابط الداخلية للعمليات الخاصة بمؤسساتهم. لقد انتهت عمليات التشغيل الحاسوبية الخاصة بمكاتب الخدمة هذه ولم يعد لها وجود في هذه الأيام، وكان ذلك حتى قبل زوال الأجهزة المركزية mainframe بفترة كافية. على كل حال فقد وقعت بعد ذلك بعض الأمور المشابهة لما يحدث هذه الأيام مع المؤسسات التي تقوم بتحويل بعض عمليات التشغيل الاعتيادية الخاصة بها إلى بيئة الحوسبة السحابية. القضية الرئيسية هي أن المؤسسات لا تقوم دائماً بتوجيه الأسئلة الملائمة لمقدمي الخدمات الخاصة بهم عندما يقومون بالتحويل إلى البيئة السحابية ذات البنية الموجهة نحو الخدمات SOA.

عند اتخاذ قرار يتعلق باختيار مقدم الخدمة كجزء أساسي من عملية الانتقال إلى البنية الموجهة نحو الخدمات SOA والحوسبة السحابية، فإن المؤسسة يجب أن تسأل كلاً من هؤلاء الباعة المتنافسين على تقديم الخدمات بعض الأسئلة الحاسمة والمهمة التي تتعلق بعمليات التشغيل والمعايير الخاصة بهم. ويجب على الفريق الإداري المسؤول عن حوكمة تقنية المعلومات في المؤسسة الحصول على ضمانات كافية بشأن بعض المجالات والمخاوف السبع التالية في عملية مزود الخدمات الحاسوبية السحابية:

١- **المستخدم المصرح له بالوصول إلى البيانات:** إن البيانات الحساسة التي تتم معالجتها خارج المؤسسة وفي بيئة الحوسبة السحابية تحمل معها مستوى متأسلاً من المخاطر، نظراً لأن خدمات التعهيد الخارجي تغفل الضوابط المادية والمنطقية وكذلك الضوابط الخاصة بالأفراد العاملين بتقنية المعلومات التي تمارسها إدارة تقنية المعلومات على برامج نظمها الداخلية وتبذل فيها الكثير من الجهد. لذا يجب على مقدم خدمة الحوسبة السحابية إعطاء معلومات وضمائم كافية تتعلق بالأشخاص الذين سيتولون إدارة بيانات ونظم المؤسسة في البيئة السحابية. كما يجب على مزودي الخدمات توفير معلومات محددة عن عمليات التوظيف والإشراف على مديري النظم أصحاب الامتيازات والصلاحيات وعن الضوابط المفروضة على وصولهم للبيانات والنظم.

٢- **الامتثال التنظيمي:** إن المؤسسة في النهاية هي المسؤولة عن أمن وسلامة بياناتها حتى بعدما تقوم برفعها إلى أحد مزودي الخدمات. لذا يجب على مقدم الخدمات الحاسوبية السحابية إعطاء معلومات تفصيلية وكافية عن السياسات الخاصة بحوكمة الأمن المتبعة لديها وعن النتائج المعلنة الخاصة بتقارير عمليات التدقيق الخارجي الأخيرة وبالشهادات المتعلقة بالأمن لديه. ويجب أن يوافق مزود الخدمة على إخطار المؤسسة بتلك الأنشطة بشكل منتظم.

٣- **أماكن البيانات:** عندما تقوم المؤسسة باستخدام البيئة السحابية لتخزين البيانات والنظم الأساسية الخاصة بها، فمن المحتمل ألا تكون المؤسسة على علم بالمكان الذي سيستضيف البيانات الخاصة بها، بل حتى بالدولة التي ستوجد بها هذه البيانات والنظم. وبموجب قوانين ملكية البيانات، فإنه يتعين على مقدمي خدمات الحوسبة السحابية تقديم معلومات كافية عن الالتزامات والاختصاصات القضائية للأماكن التي سيتم فيها حفظ ومعالجة بيانات المؤسسة. كما يجب على مقدم الخدمة أيضاً إبرام عقد إلزامي بالامتثال والالتزام بمتطلبات الخصوصية المحلية نيابة عن عملائه.

٤- **الفصل بين البيانات:** تكون البيانات عادة داخل السحابة في بيئة مشتركة بجانب بيانات خاصة بعملاء آخرين. لذا يجب على مقدم الخدمة توفير معلومات تفصيلية حول ما سيتم عمله لفصل البيانات في فترات التوقف، ويجب عليه أيضاً تقديم دليل يُثبت أن

برامج التشفير الخاصة به قد تم تصميمها وفحصها من قبل خبراء مختصين. فحوادث التشفير قد تجعل البيانات غير صالحة للاستعمال بشكل كامل، بل من الممكن أيضاً أن تجعل حتى إتاحتها عملية صعبة ومعقدة.

٥- **استرجاع البيانات:** حتى إن كانت المؤسسة لا تعلم المكان الذي توجد فيه بياناتها داخل السحابة، فإنه يجب على مزود الخدمات السحابية أن يقوم بتوثيق ما سيحدث لبيانات وخدمات المؤسسة في حال وقوع الكوارث. كما يجب عليه أن يقدم الدليل، متضمناً نتائج الفحص الخاصة به، والذي يثبت أن وسائل الاسترجاع والتعافي المستخدمة لديه قادرة على عمل نسخ طبق الأصل من البيانات والبنية التحتية للتطبيقات عبر عدة مواقع. كما يجب على الخدمة أن تؤكد ما إذا كانت لديها المقدرة على إجراء الاستعادة الكاملة وكم من الوقت ستأخذ للقيام بذلك.

٦- **دعم التحقيق والاستقصاء:** قد يكون من المستحيل حدوث أنشطة تخص التحقيق أو الاستقصاء غير الملائم أو غير القانوني في الحوسبة السحابية. حيث إنه من الصعب إجراء تحقيقات أو استقصاءات تتعلق بالخدمات السحابية على وجه الخصوص نظراً لأن عملية الدخول وكذلك البيانات للعديد من المستخدمين قد تشارك في الموقع وقد تنتشر أيضاً عبر مجموعة من الخوادم المضيفة ومراكز البيانات الدائمة التغير. لذا يجب على مقدم الخدمة إبرام عقد إلزامي لدعم أشكال محددة من التحقيقات والاستقصاءات، إلى جانب تقديم الدليل على أن مقدم الخدمة بالفعل قد قام بدعم مثل هذه الأنشطة بنجاح.

٧- **قابلية الاستمرار والتطبيق لفترة طويلة:** لا يوجد لدى المؤسسة أي ضمانات بأن مقدم خدمة الحوسبة السحابية الخاص به لن ينكسر أبداً أو يتم ابتلاعه والاستحواذ عليه من قبل شركة أكبر. على كل حال فإنه يجب على المؤسسة أن تحصل على ضمانات كافية من مقدم خدمة الحوسبة السحابية الخاص بها بأن بياناتها ستبقى متاحة حتى بعد حدوث ذلك. كما يتعين على أي مقدم خدمة تقديم الضمانات الكافية بأن المستخدمين سوف يسترجعون بياناتهم وبالصيغة التي تسمح لهم باستخدامها في التطبيقات البديلة.

تعد الحوسبة السحابية وتطبيقات البنية الموجهة نحو الخدمات SOA الخاصة بها من المجالات المتطورة والسريعة التغير. لذا فإننا نستطيع أن نتوقع رؤية المزيد من المعايير الموضوعة وأفضل الممارسات المتعارف عليها في المستقبل. وعلى الرغم من أننا قد أشرنا إلى مكاتب خدمات تقنية المعلومات التي كانت تستخدم منذ سنوات عديدة مثلاً على كيفية عدم اختيار مقدم الخدمات السحابية، فإننا نشعر بأنه كان هناك ما يكفي من الدروس المستفادة في هذا الصدد لعدم تكرار مثل تلك الأخطاء. فالحوسبة السحابية هي الموجهة المستقبلية، ويجب علينا أن ننظر إلى المزيد من الاستخدامات لهذا المفهوم في السنوات القادمة.

نظم تقنية المعلومات وافترضية إدارة التخزين:

الافتراضية هي مفهوم يعبر عن جميع وسائل التخزين المادية لتقنية المعلومات من عدة أجهزة تخزين شبكية داخل ما يبدو وكأنه وحدة تخزين واحدة يتم إدارتها من خلال وحدة تخزين مركزية. حيث يساعد التخزين الافتراضي المدير المسؤول عن التخزين في تقنية المعلومات على إنجاز مهام النسخ الاحتياطي والأرشفة واسترجاع البيانات بشكل أكثر سهولة وفي وقت أقل، وذلك عن طريق إخفاء التعقيدات الحقيقية الموجودة في شبكة أجهزة تخزين تقنية المعلومات بالكامل. وقد قدم مؤلف هذا الكتاب لافتراضية إدارة التخزين لأول مرة عام ٢٠٠٢ عندما كان عضواً في مجموعة استشارية صغيرة في شركة إي إم سي EMC التي قامت بإطلاق الممارسات الاستشارية لمكتبة البنية التحتية لتقنية المعلومات Information Technology Infrastructure Library (ITIL) (وقد تم مناقشة أفضل الممارسات المتعلقة بآيتل في الفصل السادس من هذا الكتاب). في هذا الوقت، كانت شركة EMC أحد الرواد في مجال أجهزة إدارة التخزين وكان تقديمها لمفاهيم الافتراضية يعد ابتكاراً تقنياً كبيراً. وقد أصبحت الافتراضية منذ ذلك الوقت تُستخدم على نطاق واسع كما أنها إحدى العمليات الهامة لإدارة موارد تقنية المعلومات.

ولفهم ومعرفة افتراضية تقنية المعلومات، ينبغي على المرء أن يعود مرة أخرى إلى الأيام الأولى للنظم الحاسوبية - ولاسيما الأجهزة المركزية الكبيرة mainframes التي كانت تستخدم في الماضي. فقد كانت أنظمة التشغيل لتلك الحاسبات تتحكم

في مجموعة مختلفة من الأجهزة الطرفية المتصلة، متضمناً ذلك الطابعات ومشغلات الأشرطة وما كان يطلق عليه وقتها قرص التخزين الضخم وأجهزة تشغيل الأسطوانات. وعلى الرغم من أن أنظمة الحاسبات المركزية mainframe البدائية هي التي قامت في البداية بالاستخدام المكثف لمشغلات الأشرطة الممغنطة الرخيصة نسبياً في عمليات تخزين البيانات؛ فإن التقنية سرعان ما تحولت إلى استخدام أجهزة التخزين التي اعتمدت في البداية على الأسطوانات الممغنطة الدوارة ومن ثم على مشغلات الأقراص. وعلى الرغم من الأثمان الباهظة لمشغلات الأسطوانات والأقراص عندما تم تقديمها لأول مرة في الأيام الأولى لظهور تقنية المعلومات، فإنه سرعان ما أصبحت تلك المشغلات أكثر شيوعاً واستخداماً من مشغلات الأشرطة البدائية. فقد كانت مشكلة مشغلات الأشرطة هي أنه من أجل قراءة السجل رقم ١٠٠,٠٠٠ مثلاً لابد أن يمر مشغل الشريط أولاً على ٩٩,٩٩٩ سجلاً قبله للوصول إليه. وسرعان ما أصبحت مشغلات الأسطوانات بمثابة بصمة تاريخية، وسرعان ما انتقلت التقنية إلى الأقراص الدوارة التي امتازت بالسرعة العالية وبمخططات الفهرسة التي كانت تسمح لها بتحديد موقع السجل رقم ١٠٠,٠٠٠ بشكل فوري إلى حد ما.

بوجه عام، فإن افتراضية تقنية المعلومات تعني إنشاء نسخة افتراضية من أجهزة أو موارد تقنية المعلومات، مثل الخادم، أو أجهزة التخزين، أو الشبكة، أو حتى نظام التشغيل حيث يعمل إطار العمل على توزيع هذا المورد على واحد أو أكثر من بيئات التشغيل. حتى إن الممارسة الشخصية الشائعة والخاصة بتقسيم القرص الصلب لنظام الحاسب المكتبي (الشخصي) تعد شكلاً من أشكال الافتراضية نظراً لأنك تقوم بأخذ قرص واحد وتقوم بتقسيمه إلى اثنين من مشغلات الأقراص الصلبة. حيث يستطيع كل من الأجهزة والتطبيقات والمستخدمين التفاعل مع هذا المورد الافتراضي كما لو كان مصدراً منطقياً واحداً حقيقياً. لقد أصبح مصطلح الافتراضية بطريقة ما مصطلحاً شائعاً في عالم تقنية المعلومات، وأصبح يُطلق على نظم الحاسب والعناصر التي تم تحويلها إلى البيئة الافتراضية اسم الأجهزة الافتراضية Virtual Machines (VMs). ترتبط افتراضية تقنية المعلومات بعدد من التقنيات الخاصة بتقنية المعلومات تشمل ما يلي:

• **التخزين الافتراضي Storage virtualization:** وهو دمج العديد من أجهزة التخزين الشبكي بحيث تبدو كأنها وحدة تخزين واحدة، فقد كانت المرة الأولى التي تم فيها تقديم افتراضية إدارة التخزين لتقنية المعلومات نحو عام ٢٠٠٢ من قبل شركة EMC، وقد تم التقاط هذا المفهوم من قبل العديد من بائعي المعدات الحاسوبية لنظم إدارة التخزين.

• **الخادم الافتراضي Server virtualization:** وهو تقسيم الخادم الفعلي إلى خوادم افتراضية أصغر حجماً. وقد كانت شركة IBM هي أول من طور هذا المفهوم عن طريق نظام التشغيل الخاص بالحاسب المركزي الافتراضي VM mainframe الخاص بها والذي يعود إلى ثمانينيات القرن الماضي.

• **نظام التشغيل الافتراضي Operating system-level virtualization:** وهو أحد أنواع التقنية الافتراضية للخادم التي تتعامل مع نظم التشغيل المعقدة ذات الطبقات البرمجية المتعددة.

• **الشبكة الافتراضية Network virtualization:** يمكن جعل الشبكة الفعلية الواحدة عبارة عن شبكة افتراضية من خلال عمليات التقسيم المنطقية لموارد الشبكة.

• **التطبيق الافتراضي Application virtualization:** يمكن استخدام هذا المفهوم نفسه لزيادة فائدة وكفاءة تقنية المعلومات وإدارة عمليات الترقية والنسخ الاحتياطي بصورة أكثر سهولة. وهو ما سنقوم بتوضيحه في القسم التالي.

إن الافتراضية عموماً هي فصل وظائف الجهاز عن عناصره الحقيقية باستخدام برمجيات خاصة. ففي البيئة الافتراضية يتم فصل الموقع الفعلي للوحدة عن وظائفه وتقوم برمجيات التحكم بإدارة البيانات أو الوظائف بغض النظر عن أماكنها الحقيقية. حيث تعتبر عملية إدارة وحدات مادية منفصلة والتحكم بها من خلال برنامج خاص بالافتراضية من الطرق الفعالة جداً. فباستخدام برمجية التحكم المناسبة، يمكن استخدام تقنيات البيئة الافتراضية في العديد من أجهزة ومعدات تقنية المعلومات متضمنة إدارة التخزين ومكونات الشبكة والخوادم وأنظمة التشغيل وحتى التطبيقات.

لقد اقتحمت اليوم البيئة الافتراضية لتقنية المعلومات صناعة تقنية المعلومات بكل ما تعنيه الكلمة من معنى. فقد أشارت استطلاعات الرأي إلى أن ما يزيد عن نصف إدارات تقنية المعلومات في المؤسسات الكبيرة حالياً تقوم بتشغيل خادم افتراضي واحد على الأقل، وأن هناك عدداً أقل بكثير لكن متزايد من هذه الإدارات لديها إستراتيجيات أمنية قد صُممت خصيصاً للعمل في تلك البيئة الافتراضية الخاصة بها. من ناحية أخرى، سواء كانت المؤسسة قد قامت فعلاً بتطبيق إستراتيجية البيئة الافتراضية لتقنية المعلومات أم ما زالت في طور التطبيق لها، فمن المحتمل أن تكون الشركة عرضة لمخاطر التهديدات الأمنية التي يمكن أن يكون لها تأثير كبير في البيئة التشغيلية الخاصة بالمؤسسة. ولما كانت النظم التقليدية لأمن تقنية المعلومات تعتمد على المعدات وعلى نظم التشغيل الخاصة لتقوم بحماية البيئة التي تعمل بها، فإنها تكون عديمة الفائدة في البيئة الافتراضية التي تهدف بالأساس إلى تقليل المعدات المستخدمة أو الاستغناء عنها.

هذا بالإضافة إلى أن أفضل الممارسات التقليدية أصبحت الآن في موضع شك نظراً لأن تنفيذ التجزئة المادية وغيرها من الأساليب الأخرى يعد أمراً مستحيلاً إلى حد ما في ظل تلك الممارسات. وأخيراً، فإنه نظراً لطبيعة البيئة الافتراضية، تتزايد تعقيدات الشبكة بشكل أسرع من نظم الإدارة والمراقبة القديمة، مما يجعل الرؤية فيما يتعلق بالبيئات الافتراضية والحقيقية غير واضحة تماماً. لذلك تحتاج المؤسسات إلى أن تنظر بعمق إلى الأساليب الجديدة المتبعة لتأمين شبكاتها ومعلوماتها الحساسة في العالم الافتراضي الجديد.

يناقش القسم التالي بعض القضايا الفريدة الخاصة بأمن تقنية المعلومات والمرتبطة بتطبيق البيئة الافتراضية لتقنية المعلومات، التي تتجاوز القضايا العامة لحوكمة أمن تقنية المعلومات والتي تمت مناقشتها في الفصل العاشر من هذا الكتاب. بالإضافة إلى ذلك قد تثير البيئة الافتراضية بعض القضايا الفريدة لحوكمة تقنية المعلومات. لذا يتعين على المديرين فهم إستراتيجية البيئة الافتراضية وعمليات الرقابة الداخلية لإدارات تقنية المعلومات الخاصة بهم.

حوكمة تقنية المعلومات والافتراضية:

كما ذكرنا سابقاً، كان الظهور الأول لمفهوم الافتراضية في عصر الحاسبات المركزية mainframe عندما قامت شركة IBM بطرح المفهوم الذي أطلقت عليه اسم الأجهزة الافتراضية VM Machines كأحد العناصر الخاصة في بنية الحاسبات المركزية لديها، وقد كان ذلك في ثمانينيات القرن الماضي. ثم انتقلت الخصائص الفريدة الخاصة بالأجهزة الافتراضية بعد ذلك إلى حاسبات سطح المكتب، تماماً كما انتقلنا نحن إلى النظم القائمة على بيئة الخادم-العميل ثم انتقلت إلى عالم الإنترنت. لقد أصبحت الافتراضية اليوم في مقدمة الموضوعات الساخنة نظراً لأننا نقوم بتحويل عمليات إدارة التخزين من البيئة الواقعية إلى الافتراضية وتطبيق الأجهزة الافتراضية في بيئة النظم الشبكية المتعددة الخوادم الموجودة اليوم.

لقد اعتقد مديرو مراكز البيانات بداية بأنهم يستطيعون إدارة تلك الأجهزة الافتراضية بطريقة تشبه كثيراً الطريقة التي يستخدمونها في إدارة الخوادم الحقيقية الخاصة بهم، إلا أن التجربة أثبتت استحالة هذا الأمر بشكل عام. فمع وجود العديد من القواسم المشتركة بين البيئتين الافتراضية والحقيقية، هناك أيضاً بعض الاختلافات الجوهرية التي تؤثر في إدارة وحوكمة النظم.

إن التأثير المحتمل لافتراضية إجراءات وعمليات الرقابة الموجودة والمعمول بها حالياً يعد واحداً من الاختلافات الرئيسية الكبيرة هنا. فعلى سبيل المثال، هناك مجموعة من العمليات والإجراءات المتبعة في مركز البيانات بخصوص عملية إضافة وتجهيز مجموعة من الخوادم الجديدة، ويتضمن ذلك سلسلة من التوقيعات والإجراءات المتعلقة بعمليات التسليم الموجودة بين مختلف فرق مركز البيانات، وينتج عن ذلك في النهاية خادم جديد تم تركيبه في مركز البيانات. فضلاً عن إمكان إحدى عمليات تشغيل تقنية المعلومات إنشاء خادم افتراضي جديد، حرفياً، بمجرد النقر على زر الفأرة - وذلك إما بنسخ أحد الأجهزة الافتراضية الموجودة أو إنشاء جهاز افتراضي جديد من القوالب المخصصة لذلك - وقد أصبح من السهل تجاوز مثل تلك العمليات.

على سبيل المثال يمكن لعمليات تشغيل تقنية المعلومات المؤسسية عمل عدة نسخ افتراضية متماثلة من الخادم نفسه وتوزيعها على وحدات التشغيل الموجودة في المنظمة المحيطة بها. وقد تكون هناك تحديات بالنسبة للحوكمة والرقابة في تتبع هذه النسخ. حيث ستقوم النظم الإدارية المقدمة من قبل بائعي البرمجيات الافتراضية بتحديد أماكن الأجهزة الافتراضية عند لحظة زمنية محددة، ولكنها عاجزة عن أن تحدد أين كانت أو مدى علاقتها بالخوادم الافتراضية الأخرى. ومما يزيد الأمر تعقيداً حقيقة أن الأجهزة الافتراضية، كما تم تعريفها، متحركة. فهي قادرة على الحركة حول البيئة الخاصة بها بعد أن يتم نشرها. فهذه الحركة لا تجعل عملية تتبع وإدارة تلك الأجهزة الافتراضية أكثر صعوبة فحسب، بل يمكن أيضاً أن تكشف السياسات الخاصة بتقسيم البيانات والتطبيقات.

إن هذه الاختلافات، وغيرها، تجعل من الصعب أيضاً بالنسبة لمعظم أدوات إدارة مراكز البيانات المعمول بها حالياً أن تكون قادرة على العمل في الفضاء الافتراضي وستترك العديد من النقاط المبهمة أو الغامضة. ومما يزيد هذا الأمر تعقيداً قلة الأدوات اللازمة للإدارة الافتراضية وإعداد التقارير الخاصة بها وأتمتها. وتكون النتيجة بيئة يدوية تماماً حيث لا تتكامل على نحو جيد مع نماذج الامتثال والرقابة الحالية لمركز البيانات. وهذا يعني أن نظم "الراية الحمراء" أو التنبيه التقليدية قد لا تتمكن من العمل بالشكل المناسب في هذا الفضاء (الافتراضية)، فهي إما أن يتم التحايل عليها وإما أنها ببساطة لا تستطيع رؤية عمليات التشغيل اليومية، فتترك مراكز البيانات مكشوفة أو مستهدفة.

في مركز البيانات الفعلي الخاص بتقنية المعلومات وبجميع ما يتضمنه من نظم وعمليات وضوابط وتوازنات رقابية، يتم إصدار التنبيهات في حال حدوث أمور خارجة عن المألوف. فالإدارة ومن خلال الاستثناء تكون هي القاعدة المتبعة اليوم وهي البيئة التي تعتبر عدم وجود أخبار جديدة هو بحد ذاته خبراً جيداً. لكن البيئة التي تكون فيها الضوابط اليدوية هي المهيمنة غالباً وتشح فيها عمليات التبليغ عن الأحداث، وقصور الرؤية الرقابية قد تؤدي إلى إيجاد قضايا لن تستطيع إدارة عمليات تشغيل تقنية المعلومات التنبؤ بها مستقبلاً. وقد لا تعد قضية ضخمة بالنسبة لبيئة الحوسبة الافتراضية الصغيرة، ولكن كلما نمت البيئة وازداد حجمها، نمت معها أيضاً آثار تلك القضايا.

عندما تقوم إدارات تقنية المعلومات المؤسسية بتبني تلك البيئات الافتراضية، فإن نقص الضوابط الآلية في بعض بيئات الأجهزة الافتراضية والحاجة المتزايدة لأنشطة الضوابط الداخلية اليدوية قد يتسبب في حالة من عدم التوازن بين عمليات التشغيل الخاصة بتقنية المعلومات وعمليات التشغيل الخاصة بالضوابط الداخلية. وسوف تتفاقم هذه الحالة (حالة عدم التوازن) فقط عندما تنمو بيئة الأجهزة الافتراضية. إن هذا النقص في الضوابط الآلية، والمتابعة، والقياس المستمر في مراكز البيانات الافتراضية، إضافة إلى زيادة العمليات اليدوية المصاحبة، أدى إلى استحداث بيئة تحتوي على ضوابط ذات فاعلية أقل ومخاطر أكثر من البيئة الحقيقية المناظرة لها.

قضايا حوكمة وأمن البيئة الافتراضية لتقنية المعلومات:

عندما ينتقل التخطيط الذي يُبذل فيه جهد كبير ولكنه في النهاية يخرج بشكل سيئ إلى البيئة الافتراضية، فإنه قد يتسبب في إيجاد تحديات بالنسبة للمؤسسة. وكما ناقشنا في الفصول الأخرى، كلما خرج المزيد من الأنظمة الموضوعة للحوكمة، وإدارة المخاطر، والامتثال (GRC) عن التوازن، زاد التأثير في الأعمال بصورة كاملة. إن "نقاط التحول" الفردية هنا ستكون مختلفة لكل مؤسسة على حدة، ولكن عاجلاً أو آجلاً سيتم الوصول إليها، وذلك عندما تبدأ المؤسسات في رؤية التصاعد المستمر في تكاليفها ومخاطرها. وربما يكون هناك العديد من المؤسسات التي تعمل حالياً في ظل وجود نفقات غير مخطط لها على تقنية المعلومات، وذلك بسبب انتقالها إلى بيئات افتراضية غير فعالة. في حين تشهد مؤسسات أخرى ارتفاع نسبة الحوادث المرئية وغير المرئية في مراكز البيانات. جميع هذه الأمور ستؤثر في نهاية المطاف على مجمل أداء الأعمال المؤسسية.

ينبغي على المدير الأول في المؤسسة أن يناقش إستراتيجيات البيئة الافتراضية والأجهزة الافتراضية لتقنية المعلومات مع إدارة تقنية المعلومات. فإذا بدا أن الانتقال إلى الأجهزة الافتراضية سيكون على النحو المتفق عليه، فإنه يجب أن يكون هناك دليل على وجود خطة قوية لهذا المشروع (مشروع الانتقال)، كما تمت مناقشته في الفصل السادس عشر من هذا الكتاب، هذا بالإضافة إلى وجود تقدير واضح لبعض المخاوف الاستثنائية للرقابة المرتبطة بالبيئة الافتراضية لتقنية المعلومات. ولا يزال هناك العديد من السياسات التشغيلية

وسياسات المخاطر والأهداف الرقابية يمكن تطبيقها في العالم الافتراضي. ربما يكون قد تم ضبطها لتتناسب مع الطبيعة الحركية لتلك البنية الجديدة، لكنها لا تزال تُطبق. وذلك يشمل العناصر المشتركة بالنسبة لجميع الخوادم (حقيقي أو افتراضي) كالتهيئة، وإدارة التوصيلات (التوصيلات الكهربائية)، والأمن. من ناحية أخرى، فإن للبيئة الافتراضية تفرداً يتطلب سياسات وضوابط جديدة تشمل ما يلي:

- **إدارة الهوية Identity management:** نظراً للطبيعة الحركية للأجهزة الافتراضية، ستكون هناك حاجة إلى مستوى ما لإدارة هوية الملفات والموارد التي لا تعتمد على (الأعراف) البسيطة للتسمية. لذا يتعين على وحدة ضمان جودة تقنية المعلومات إلى جانب التدقيق الداخلي لتقنية المعلومات، مراجعة وتقييم العمليات من أجل ضمان تطبيق السياسات بشكل سليم.

- **التحكم في تنقلية الجهاز الافتراضي VM mobility control:** أحد العناصر الأساسية في القيمة المضافة بالنسبة للبيئة الافتراضية هو المرونة التي قدمتها لمجموعات تقنية المعلومات. فقد تم تصميم الأجهزة الافتراضية بحيث تكون متحركة وتستطيع بكل سهولة الانتقال من خادم إلى آخر، سواء كان ذلك استجابةً للعمليات الآلية لتوازن الأحمال، أم بسبب الإزالة اليدوية للأجهزة الافتراضية من أحد الخوادم الحقيقية التي تحتاج إلى صيانة. من ناحية أخرى، فإن هذه المرونة يمكن أن تكون سلاحاً ذا حدين، وذلك عندما لا يجب أن تكون جميع الأجهزة الافتراضية متنقلة. فعلى سبيل المثال، قد تحتاج إدارة تقنية المعلومات، سواء لأهداف تتعلق بالرقابة أم بالتدقيق، إلى إثبات أن تطبيقاً ما متفق مع اللوائح التنظيمية أو المعايير الداخلية للشركة. فربما يكون هناك حاجة لسياسات تتعلق بالأماكن التي يجب والتي لا يجب أن تعمل بها بعض الأجهزة الافتراضية المحددة، كما تتعلق أيضاً بتحديد المدة الزمنية التي يُسمح بها ببقاء الأجهزة الافتراضية دون اتصال.

- **التزويد الاحتياطي Provisioning:** يمكن التحايل بسهولة على العمليات التقليدية المتبعة لإضافة خادم جديد. لذا لا بد من وضع عمليات جديدة تحكم كلاً من: ما الذي سيتم التزود به؟ (ما الذي سيتم إنشاؤه احتياطياً؟)، ومن الذي يملك سلطة السماح بإضافة خوادم جديدة؟

• **فصل البيانات Data separation:** لكل مركز بيانات مجموعة من القواعد المتبعة للقيام بعملية الفصل بين بيانات التطبيقات لديه، والتي يكون الدافع لها عادة إما المخاوف الأمنية أو القضايا المتعلقة بالامتثال. فعندما تقوم إدارة تقنية المعلومات بوضع التطبيقات في البيئة الافتراضية والتي تندرج تحت هذه المعايير، فمن المهم التفكير في الكيفية التي سيقرب بها هذا الأمر على الجانب الافتراضي، ولكن أيضاً للحماية من التحركات غير الملائمة المقصودة وغير المقصودة خلال دورة حياة هذا الخادم.

• **الاسترداد Reclamation:** إن ضمان إزالة الأجهزة الافتراضية الزائدة أو غير المستخدمة يعد مجالاً آخر من المجالات التي تتطلب سياسة وأهدافاً معينة. كما أن الآثار الأمنية المترتبة على هذه التقنية الجديدة هي أيضاً بحاجة إلى أن تؤخذ بعين الاعتبار، وهي تشمل: تأثير الأجهزة الافتراضية على النظم الأمنية لتقنية المعلومات المعمول بها حالياً (فبعض النظم لا تعمل جيداً في البيئة الافتراضية)، ومدى احتمالية التعرض لتهديدات هجومية جديدة.

قد لا يكون المدير التقليدي المسؤول عن حوكمة تقنية المعلومات المؤسسية مُلمّاً بتلك القضايا والمسائل السابقة الذكر. ومع ذلك، قد تُستخدم تلك المسائل نقاط حوار رئيسية خلال الحديث مع إدارة تقنية المعلومات لديهم حول ما يتعلق بتقييم أي برنامج يخص افتراضية تقنية المعلومات داخل المؤسسة. وعلى الرغم من سرعة تبني الخادم الافتراضي في جميع أنحاء العالم، فإنها لاتزال تقنية غير ناضجة نسبياً. فبالنسبة للكثيرين قد دخل الخادم الافتراضي إلى مركز البيانات من الباب الخلفي كأحد الأدوات التشغيلية المستخدمة والتي حققت مستوى جيداً من العوائد الاستثمارية (Return On Investment (ROI، وقد تطور الخادم الافتراضي منذ ذلك الوقت ليصبح البنية الهيكلية الجديدة لمركز البيانات. لكن دخوله بهذه الطريقة جعله لا يخضع أبداً للعمليات الاعتيادية الخاصة بمراجعة الضوابط الداخلية التي يتم اتباعها عادة من قبل إدارات تقنية المعلومات قبل إطلاق الخوادم في مركز البيانات، وأسهم دخول الخادم الافتراضي بهذه الطريقة أيضاً في نقص بعض الوظائف التي تشتد الحاجة إليها.

يوجد في السوق اليوم عدد من منتجات منصات البرمجيات الافتراضية ، وتعتبر في إم وار VMware هي الشركة الرائدة في هذا المجال، مع وجود عدد قليل من الشركات الأخرى مثل شركة مايكروسوفت Microsoft وشركة سيطركس Citrix. فكل منصة من هذه المنصات مجموعة مختلفة من نقاط الضعف ونقاط القوة، وقد خلصت العديد من إدارات تقنية المعلومات إلى تشغيل خليط مكون من تلك المنصات الثلاث معاً، الأمر الذي أثار قضية أو مشكلة تتعلق بكيفية إدارة تلك البيئات غير المتجانسة. فليس بالأمر المفاجئ أن تركز نظم الإدارة المُقدمة من قبل باعة النظم الافتراضية على نقل الجهاز الافتراضي أكثر من تركيزها على إدارة البيئة نفسها. إضافة إلى ذلك فإن معظم باعة النظم التقليدية الخاصة بإدارة مراكز البيانات يملكون نظاماً تم بناؤها للعمل في بيئة مراكز البيانات الحقيقية ولا تعمل جيداً في البيئات الافتراضية.

واعتماداً على عمليات تشغيل تقنية المعلومات وعلى العمليات الخاصة بالحوكمة وإدارة المخاطر والامتثال GRC التي تمت مناقشتها في فصول أخرى، فإنه ينبغي على إدارة المؤسسة العمل مع عمليات تشغيل تقنية المعلومات لديها لمعرفة ما إذا كانت المعايير المناسبة الخاصة بالرقابة الداخلية لا تزال موجودة ومعمولاً بها في البيئة الافتراضية. فبالنسبة للكثيرين ربما يكون هناك حاجة لنظم إضافية في مراكز البيانات الافتراضية، سواء كان ذلك لتعويض القصور الموجود في نظم إدارة مراكز البيانات والبيئات الافتراضية المعمول بها حالياً أم لفرض وتطبيق سياسات إضافية يتطلبها هذا المجال.

لقد وُجدت البيئة الافتراضية هنا لتبقى. لذلك إذا كثفت إدارة تقنية المعلومات من تبنيها للخوادم الافتراضية في مركز البيانات الخاصة بها، فإنه يجب عليها أن تأخذ بعين الاعتبار آثار استخدام تلك الخوادم الافتراضية على الضوابط الداخلية للأعمال والتي تتضمن ما يلي:

- تطبيق المعايير والعمليات المعمول بها حالياً في الفضاء الافتراضي أينما أمكن: من المحتمل أن تحتاج المعايير والعمليات المعمول بها حالياً إلى تعديلات، ولكن مع التأكيد على وضعها موضع التنفيذ لتبدأ بتقديم الرؤية والرقابة المطلوبة بالإضافة إلى التبصر فيما هو ضروري ومطلوب من نظم إدارية إضافية.

• وضع المعايير والعمليات الجديدة التي تحتاج إليها تلك التقنية: ينبغي على المؤسسة أن تزيد من مستوى رقابتها إلى ما هو أبعد من ذلك، وعلى الأقل يجب أن تشمل هذه الأمور على:

- المراقبة والتبليغ.
- التحكم في التزويد التقني.
- إدارة هوية الجهاز الافتراضي.
- ضبط تنقلية الأجهزة الافتراضية لفرض الفصل بين البيانات.
- إصلاح الأجهزة الافتراضية عند انتهاء العمر الافتراضي لها.

• الأتمتة قدر الإمكان: إن العمليات اليدوية ليست متناغمة وتحتاج إلى المزيد من الوقت لإتمامها. لذا سنجد في نهاية المطاف أن الطريقة الوحيدة لإعادة التوازن لنموذج الحوكمة وإدارة المخاطر والامتثال GRC هو زيادة مستوى التشغيل الآلي عن طريق تطبيق نظم إضافية جديدة يحتاج إليها هذا المجال. وهذا سيكون له تأثير إضافي من أجل الحد من النشاط والعمليات اليدوية، وزيادة الضوابط الداخلية، وتقليل المخاطر، إضافة إلى توفير كميات كبيرة من الوقت المستهلك في العمليات الإدارية.

• مراجعة البنية الأمنية لديك: لكي نكون أكثر كفاءة وفاعلية، فإن العديد من أنواع الأجهزة الأمنية والأدوات الرقابية التي نود أن نعرف ما الذي تقوم بحمايته هذه الأجهزة وأين يكون، وكذلك حركة الأجهزة الافتراضية؛ كل ذلك قد يكون محل جدال. وقد يفرض التغيير المستمر الموجود في البيئة الافتراضية مطالب حيوية ديناميكية على أي نوع "ثابت" من أنواع الحلول الأمنية وحتى في البنى التحتية للبيئات الافتراضية الصغيرة. خلاصة القول هي: أن بعض البنى التحتية الأمنية لن تعمل جيداً في البيئة الافتراضية، وربما يكون المنتج الأمني، غير القادر على العمل جيداً على مستوى جميع الأهداف والممارسات، غير قادر أيضاً على العمل مطلقاً.

• تطبيق معايير تدقيق ومعايير داخلية محددة (ونظم إبلاغ) تناسب الفضاء الافتراضي: فكما وضعنا سابقاً، إن البيئة الافتراضية تحتاج إلى سياسات وممارسات ومعايير رقابية

جديدة. وعند دخولها حيز التنفيذ، ستحتاج أيضاً إلى رقابة داخلية، وعمليات تدقيق، وإجراءات جديدة مناظرة لها. فعلى سبيل المثال، تحتاج التطبيقات الممتثلة لقانون SOx إلى أن تكون مفصولة عن النظم الأخرى، وتحتاج أيضاً إلى تطبيق ضوابط أكثر صرامة على عمليات الوصول للبيانات. إلا أن التنقلات الطبيعية للخوادم الافتراضية أسهمت في إضافة عامل جديد إلى عملية التدقيق وهو: هل تم انتقال هذا الجهاز الافتراضي إلى أحد الخوادم الإضافية خلال الفترة الزمنية المخصصة لعملية التدقيق؟ إذا كان هذا قد تم، فما الأجهزة الافتراضية الأخرى التي كانت موجودة على هذا الخادم؟

وكما يحدث عادة مع أي تقنية جديدة تخص تقنية المعلومات، قد يتسبب تركيب برمجيات البيئة الافتراضية وكذلك التغييرات الكبرى في إحداث بعض التحسينات الجوهرية على مستوى كفاءة العمليات. على أي حال، فإن إدارة تقنية المعلومات هي من تقوم غالباً بتنصيب تلك الأدوات الجديدة، غير أنها تتجاوز غالباً مستوى فهم الإدارة العامة العليا، لذا يجب أن يحصل كبار المديرين، على جميع المستويات، على فهم عام حول نشاطات البيئة الافتراضية في مؤسساتهم.

يوضح الشكل التوضيحي (٩-٢) قائمة ببعض الممارسات الجيدة لحوكمة تقنية المعلومات في البيئة الافتراضية لإحدى المؤسسات التجارية التقليدية. إذ يجب أن تساعد هذه الممارسات المدير الأول على فهم الكيفية التي من خلالها يتم تطبيق البيئة الافتراضية في المؤسسة.

لقد بدأ العمل بالبيئات الافتراضية في معظم مراكز البيانات على أنه جهد تخطيطي، قاده قسم تقنية المعلومات، وقد ركز وقتها على مسألة الفوائد العائدة من الاستثمارات ROI الخاصة بعملية دمج الخوادم. لكن الانتقال من تكامل الخوادم الذي كان يتم لتحقيق غرض معين إلى البيئة الافتراضية أدى إلى المزيد من الاستخدامات في بيئة العمل الإنتاجية، وزيادة نسبة مراكز البيانات ذات البيئة الافتراضية، كل ذلك يتطلب نظرة أكثر إستراتيجية حول مدى تأثير هذه البنية في إدارة مراكز البيانات والضوابط الخاصة بالأعمال. فوجود ممارسات وعمليات فعالة تتعلق بالبيئة الافتراضية سيضمن قدرة المؤسسة على تحسين القيمة الإجمالية لهذه التقنية.

شكل توضيحي (٩-٢)

الممارسات الجيدة لحوكمة تقنية المعلومات في البيئة الافتراضية

- **التأكد من أن جميع الأطراف المتأثرة تدرك مزايا وعيوب البيئة الافتراضية:** قبل انتقال تقنية المعلومات من النظم الفعلية القديمة إلى النظم الافتراضية، أو القيام بإضافة مجموعة جديدة من الخوادم الافتراضية لتنفيذ أعباء أعمال محددة، فإنه ينبغي على إدارة تقنية المعلومات والإدارة أن يتأكدوا من فهمهم للقيود والحقائق المتعلقة بالبيئة الافتراضية من حيث استخدامات وحدة المعالجة المركزية والذاكرة ومجمل الضوابط الخاصة بحوكمة تقنية المعلومات.
- **تحديد الأولويات لإدارة النظم الافتراضية وتصحيحها وأمنها:** أي وضع قيود على عملية انتشار الأجهزة الافتراضية، وتشمل جميع الأجهزة الافتراضية الموجودة في حزم تقنية المعلومات، والإدارة، والبنى التحتية الخاصة بسياسات الأمن.
- **التعامل مع النظم الافتراضية كما لو كانت نظاماً فعلية في معظم الأحوال:** بشكل عام فإنه يجب ألا تُعامل النظم الافتراضية كما لو كانت مختلفة عن أي من النظم الفعلية. لذا يجب أن يتم تطبيق النظم الافتراضية وفقاً لمجموعة معرفة على نحو جيد من البيانات الخاصة بسياسات وممارسات الحوكمة والتي صُممت بالشكل الذي يضمن أن بيانات النظم الافتراضية:
 - o **يمكن الوصول إليها:** بمعنى أنه يجب أن يتمكن مستخدمو النظم الافتراضية من الوصول إلى البيانات التي يحتاجون إليها وبالصيغ التي تتوافق مع متطلباتهم.
 - o **آمنة:** تماماً كما هو الحال بالنسبة لجميع التطبيقات الاعتيادية، فقط الأشخاص المصرح لهم هم الذين يجب أن يُسمح لهم بالوصول إلى بيانات النظم الافتراضية، أما الأشخاص غير المصرح لهم بذلك فيجب أن يتم منعهم من الوصول إلى تلك البيانات.
 - o **متطابقة ومتناغمة:** عندما يقوم اثنان من المستخدمين بالبحث عن البيانات نفسها، يجب أن يتم ترشيدها "نفس" البيانات في إصدارات متعددة بصورة منتظمة.
 - o **عالية الجودة:** يجب أن تكون البيانات الصادرة عن تطبيقات البيئات الافتراضية دقيقة ومتطابقة لتلبية معايير تقنية المعلومات المعمول بها.
 - o **قابلة للتدقيق:** يجب أن يكون في البيئة الافتراضية مسارات واضحة تشير إلى مصادر البيانات، ورؤية واضحة لأصل هذه البيانات، وضوابط تدل على أن إدارة تقنية المعلومات تعلم من الذي يستخدم هذه البيانات وما الغرض من استخدامها؟

• **توظيف إجراءات نسخ احتياطي قوية للتطبيقات:** إن عمل نسخ احتياطية لكامل الجهاز الافتراضي يحتاج إلى وقت أكبر ويعطي القليل من الخيارات فيما يتعلق بعملية الاسترجاع السريع للنظم. ومع ذلك، فإنه يجب أن تقوم إدارة تقنية المعلومات بعمل نسخ احتياطية وبشكل منتظم من تطبيقات البيئة الافتراضية تماماً كما لو كان يقوم بحماية النظم الفعلية ذات المهام الحساسة، والتأكد من قدرة إدارة تقنية المعلومات على تنفيذ عمليات التعافي السريعة وزيادة الثقة بالتطبيقات كذلك.

• **التخزين المركزي للنظم:** السبب الرئيسي وراء زيادة الأجهزة الافتراضية غالباً هو انتشار أجهزة الخوادم المضيفة الفعلية في جميع أنحاء المؤسسة. لذلك وفي ظل وجود النظم الافتراضية، فإن عملية نسخ كامل لنظام الضيف (أو الاثنين) سهلة جداً، وإن هذه السهولة هي السبب الرئيسي في تزايد الأجهزة الافتراضية وكذلك النتيجة المحتملة لفقدان البيانات. فإذا عجزت إدارة تقنية المعلومات عن تأمين الأجهزة الافتراضية التي لديها، فلا بد أن يكون لديها أقراص مشفرة حقيقية أو افتراضية لضمان عدم فقدان البيانات السرية. فعندما تقوم بوضع أجهزة الخوادم المضيفة الافتراضية الخاصة بك والوحدات التخزينية في أماكن مركزية آمنة، فإن إدارة تقنية المعلومات ستتمكن من الحد من تزايد الأجهزة الافتراضية وكذلك احتمالية فقدان البيانات.

قضايا حوكمة الهواتف الذكية وأجهزة تقنية المعلومات المحمولة:

يستخدم الناس هذه الأيام وعلى اختلاف مستوياتهم أجهزة الهواتف الذكية والحاسبات اللوحية لممارسة النشاطات الشخصية والمنزلية الخاصة بهم. وقد بدأ ذلك على شكل هواتف خلوية شخصية صغيرة وتطور الأمر على مر السنين إلى أجهزة قادرة على الاتصال بالإنترنت، وإرسال الرسائل النصية، والتقاط الصور وإرسالها وما هو أكثر من ذلك بكثير. يمتلك الحاسب اللوحي Tablet الإمكانات الموجودة في الحاسب الشخصي المحمول Laptop باستثناء لوحة المفاتيح الأكبر حجماً، فالحاسبات اللوحية أصغر حجماً، وأخف وزناً، وقادرة بالأساس على العمل كما لو كانت هواتف ذكية. وعلى الرغم من الميزات القوية والعديدة الموجودة في تلك الأجهزة، فإنها تعتبر نسبياً ذات تكلفة أقل. وقد أصبحت أجهزة شخصية تستخدم من قبل العديد من العائلات ومن ضمنهم الأطفال الصغار. وقد أشرنا في هذا القسم إلى جميع هذه النظم باسم الأجهزة المحمولة handheld devices، سواء كانت هواتف ذكية، حاسبات لوحية، أجهزة تخزين صغيرة USB أم غيرها.

منذ عدة سنوات ليست بالكثيرة لم تكن هذه الأجهزة المحمولة مستخدمة في أماكن العمل. إلا أن المؤسسات قد قامت بتشجيع الموظفين الرئيسيين لديها باستخدام أجهزة الحاسبات الشخصية المحمولة Laptop، وقامت بإصدار روابط آمنة لتمكينهم من الوصول إلى المنتجات البرمجية الخاصة بالمؤسسة. فضلاً عن أن تلك الحاسبات الشخصية المحمولة Laptops كانت تعار للموظفين ليقوموا باستخدامها لأغراض العمل فقط، أما الاستخدامات الشخصية لها فقد كانت غير محبذة ولا ينصح بها، وكان الموظفون يقومون بإعادة تلك الأجهزة إلى إدارة تقنية المعلومات بعد رحيلهم.

إن الاستخدام الشخصي للموظفين للهواتف الذكية والأجهزة اللوحية هذه الأيام قد يثير بعض القضايا المتعلقة بحوكمة تقنية المعلومات. فعلى سبيل المثال، تمتلك هذه الأجهزة عموماً ميزة الكاميرا الرقمية المدمجة فيها. وبالتأكيد يمكن أن يثير هذا الأمر مسألة أمنية على اعتبار أن الموظف يستطيع بسهولة التقاط صور لوثائق مهمة ومن ثم نقلها واستخدامها لأغراض غير مشروعة. فعلى الرغم من القوانين الصادرة والتي تمنع مثل تلك الممارسات، فإن المؤسسة في الواقع لا تستطيع منع مثل تلك الممارسات المتعلقة بالتصوير الداخلي بالرغم من التصريحات السياسية القوية ضد أنشطة كهذه. وكذلك الأمر بالنسبة لأجهزة التخزين الصغيرة USB المستخدمة من قبل العديد أيضاً، والتي يمكن توصيلها بأحد أجهزة الشركة لأخذ معلومات هامة وحساسة.

ترتبط العديد من المخاوف المتعلقة باستخدام الأجهزة المحمولة في أماكن العمل بالأمن المؤسسي. فالمؤسسة ستكون مضطرة للسماح لأشخاص أساسيين للقيام بالاتصال بشبكات البيانات والتي تعد جزءاً من مسئوليات عملهم. فضلاً عن أن، هناك حاجة لتنصيب برامج الجدران النارية والبرامج المضادة للفيروسات والأدوات البرمجية لمراقبة الأمن على أي جهاز نقال سوف تُعطي له صلاحية الوصول للنظم الشبكية المؤسسية. ونظراً لكثرة أنواع الأجهزة الموجودة في المؤسسة واختلاف أنواعها، فلن تستطيع المؤسسة ضبط عملية إصدار أجهزة كهذه، إلا أنها يجب أن تمتلك مجموعة من المعايير المثبتة واللازمة لضبط استخدام الأجهزة النقالة قبل السماح لها بالوصول إلى بيانات الشركة.

الشكل التوضيحي (٣-٩) يعد مثلاً على سياسة الشركة فيما يتعلق باستخدام الأجهزة المحمولة من قبل الموظفين وأصحاب المصالح في بيئات العمل. يجب أن يتم إبلاغ جميع الموظفين الجدد بمثل هذه السياسة إلى جانب مطالبتهم بقبولها بشكل رسمي. ولأن التقنية دائمة التغير، فمن الممكن أن تختلف اتجاهات وطبيعة الجهاز المحمول اليوم عما ستكون عليه غداً. لذلك فإن هذا النوع من بيان السياسة يجب أن يُعدل ويُعاد إصداره بشكل دوري ومنتظم مع ضرورة مطالبة المتلقين لتلك السياسة بالإفصاح عن فهمهم وقبولهم لتلك السياسة المنقحة. يجب أن تُستخدم العناصر الأساسية في هذه السياسة الخاصة بالأجهزة المحمولة من قبل الإدارة والتدقيق الداخلي على أنها جزء من مراجعاتهم المنتظمة للرقابة الداخلية.

شكل توضيحي (٣-٩)

سياسة استخدام الموظفين وغيرهم من أصحاب المصالح للأجهزة المحمولة

مقدمة: إن استخدام الأجهزة المحمولة في بيئات عمل شركتنا في ازدياد، وهي تقدم خدمات الأجهزة النقالة والاتصال المستمر بالأجهزة النقالة للعاملين. ونظراً لحقيقة أن الأجهزة المحمولة تكون غالباً ممتلكات شخصية لأصحابها. فهي تشكل تهديدات جديدة لأصول الشركة. وتشمل الأجهزة المحمولة التي تحمل تحديات أمنية كلاً من الحاسبات الشخصية المحمولة ووحدات التخزين المتحركة (مثل جهاز USB) والهواتف الذكية والحاسبات اللوحية وغيرها من الكاميرات.

الغرض والنطاق: تضع هذه السياسة الأمنية قواعد تتعلق بالاستخدام الصحيح للأجهزة المحمولة في جميع أنحاء الشركة، وذلك من أجل حماية سرية البيانات الحساسة، وسلامة كل من البيانات والتطبيقات، وإتاحة خدمات شركتنا. إن هذا من شأنه أن يحمي الأجهزة المحمولة ومستخداميها بالإضافة إلى أصول الشركة (سريتها وسلامتها) واستمرارية الأعمال (إتاحتها).

وتُطبق هذه السياسة على جميع الموظفين، والاستشاريين، والموردين، والمقاولين والطلاب وغيرهم ممن يستخدمون الأجهزة المحمولة النقالة الخاصة أو المرتبطة بالأعمال داخل أي مبنى من مباني شركتنا.

إن الالتزام بهذه المتطلبات وبالسياسات الأمنية المنبثقة منها والأحكام التنفيذية يعد أمراً ملزماً في جميع أنحاء شركتنا وفروعها وغالبية ممتلكاتها. و يعتبر التعدي المقصود على هذه السياسات أو الإهمال فيها تهديداً لمصالح شركتنا وسيؤدي إلى عقوبات صارمة وظيفية كانت أو قانونية أو كليهما معاً. وستطبق أيضاً هذه الشروط والسياسات الأمنية المنبثقة منها والأحكام التنفيذية على جميع الموردين التابعين لشركتنا.

الأدوار والمسؤوليات: إن جميع الموظفين وأصحاب المصالح مسؤولون عن التقيد بهذه الأحكام الأمنية. وقد تم توثيق المهام المحددة عند تعريف الأدوار، ويجب تحديد شخص بالاسم لكل دور من هذه الأدوار وأن يكون معروفاً بالنسبة لإدارة أمن تقنية المعلومات.

المسؤوليات المتعلقة بحوكمة تقنية المعلومات:

- أصحاب وحدات الأعمال: ضمان تزويد إدارة تقنية المعلومات بالمصادر الضرورية.
- إدارة تقنية المعلومات: المحافظة على السياسات الأمنية:
 - مسؤولية عن إيجاد سياسات أو تبني السياسات المعمول بها وصيانتها لمواكبة العصر.
 - تطبيق التوجيهات والإجراءات اللازمة لتنفيذ هذه السياسة وتقوم بتبليغها للأشخاص المعنيين.
 - تضمن أن جميع الإجراءات القابلة للتطبيق موثقة وتم إيصالها بشكل جيد.
 - مسؤولية عن فرض السياسة وضمان أن المستخدمين قد تلقوا التدريبات الملائمة.
- إدارة أمن تقنية المعلومات: مسئولية عن إدارة جميع الأجهزة المحمولة النقلة التي يتم إصدارها:
 - تقوم بإدارة مستودع الأجهزة المحمولة المسجلة.
 - تضمن أن الخدمات الضرورية متاحة للمستخدمين وتقوم بتقديم الموارد الضرورية لاستخدام تلك الخدمات.
 - مسؤولية عن فرض السياسة:
 - o من خلال ضوابط العمل المناسبة.
 - o تقديم طلبات تتعلق بالتغيرات الضرورية في هذه السياسة لدعم حوكمة تقنية المعلومات.
- المستخدمون وغيرهم من أصحاب المصالح: يجب على موظفي المؤسسة وأصحاب المصالح أن يقوموا بقراءة هذه السياسات الأمنية وفهمها والموافقة عليها، ويجب عليهم أيضاً إعلام إدارة تقنية المعلومات بالمخالفين لهذه السياسات الأمنية.

ملاحظة:

1. SAS 70, "Service Auditors Reports," http://sas70.com/sas70_reports.html

الفصل العاشر

الحوكمة وإدارة أمن تقنية المعلومات وإدارة الاستمرارية

تعد العمليات الفعالة والخاصة بإدارة أمن تقنية المعلومات واستمراريتها من العناصر الهامة للحوكمة الشاملة لتقنية المعلومات المؤسسية. إن أمن تقنية المعلومات مصطلح واسع، فهو يشير إلى العمليات والضوابط اللازمة لحماية كل من النظم والبيانات الخاصة بتقنية المعلومات بالإضافة إلى الأصول المادية في المؤسسة من مجموعة واسعة من التهديدات المحتملة. ففي عالمنا اليوم القائم على الإنترنت، إضافة إلى المخاطر القادمة من أشخاص من جميع أنحاء العالم ربما يكونو مُولعين بالوصول غير المشروع للأنظمة المؤمنة، أصبحت قضية أمن تقنية المعلومات الآن تحظى بالاهتمام بل وتزايد الاهتمام بها أكثر من أي وقت مضى. لذا فإن المؤسسات تحتاج إلى تطبيق عمليات فعالة خاصة بأمن تقنية المعلومات للتحكم في أصول تقنية المعلومات الخاصة بها وضبطها.

وعلى الرغم من أهمية عمليات الأمن الموضوعة لحماية الأصول الخاصة بتقنية المعلومات من الأشخاص غير المصرح لهم، فإن عمليات التشغيل الخاصة بتقنية المعلومات أيضاً تواجه تهديدات من مخاطر مثل: اندلاع حريق في أحد المرافق، أو كوارث طبيعية، أو أعطال المعدات. وقد كان يعرف هذا المجال الخاص بالمخاوف المتعلقة بمخاطر تقنية المعلومات بالتخطيط للتعافي من كوارث تقنية المعلومات IT disaster recovery planning وذلك في الأيام الأولى لظهور تقنية المعلومات عندما كانت نظم الحاسبات المركزية mainframe هي المهيمنة، أما اليوم فهي بشكل عام تسمى تخطيط استمرارية تقنية المعلومات IT continuity planning. لذا يجب على المؤسسة امتلاك الموارد اللازمة لعمل النسخ الاحتياطية، سواء كانت لمعدات أم لبرمجيات، وذلك لاستمرار العمليات التشغيلية المنتظمة والمجدولة في حال حدث أي انقطاع غير طبيعي لها.

يناقش هذا الفصل السؤال التالي: لماذا يعد وجود عمليات معمول بها لأمن واستمرارية تقنية المعلومات أمراً في غاية الأهمية بالنسبة للحوكمة الفعالة لتقنية المعلومات؟ تكون العمليات الفعالة لتخطيط أمن واستمرارية تقنية المعلومات معقدة غالباً وتحتاج إلى

مهارات المتخصصين. لذا يجب على المدير الأول الذي يعمل على توجيه ومراجعة حالة جميع عمليات حوكمة تقنية المعلومات أن يتمتع بقدر معين من المعرفة الأساسية نوعاً ما لبعض الأدوات والإجراءات الفعالة المستخدمة في هذا المجال. ومع أن كلاً من هذه الأدوات والإجراءات يعتبر من المجالات المتخصصة، فإنها أيضاً تعتبر من العناصر الهامة والضرورية للحوكمة الشاملة الفعالة لتقنية المعلومات في المؤسسة.

أهمية البيئة الفعالة لأمن تقنية المعلومات:

لقد تغير مفهوم أمن تقنية المعلومات كثيراً على مر السنين وأصبح أمراً أكثر تعقيداً. فبالعودة إلى عصر نظم الحاسبات المركزية، كنا نعتقد أن أمن تقنية المعلومات لا يتعدى أنظمة بسيطة لكلمة المرور ووضع أقفال على أبواب مركز الحاسب. وقد كان من المهم في ذلك الوقت أن تكون أصول تلك النظم محمية ويتم عمل نسخ احتياطية لها بشكل متكرر. وكانت تقع مسؤولية تلك العمليات على عاتق وحدة أو إدارة عمليات تشغيل تقنية المعلومات مع تدخل محدود من قبل الإدارة العامة.

أما في هذه الأيام، وفي ظل تكرار النشرات الإخبارية حول تلك الأحداث المتعلقة بتقنية المعلومات كسرقة ملفات النظم الحاسوبية الخاصة بالبطاقات الائتمانية، أو إفشاء ما هو من المفترض أن يكون ملفات لرسائل سرية خاصة بنظام الحاسب، أصبحت قضايا أمن تقنية المعلومات مسألة هامة بالنسبة للعديد من أعضاء فريق تقنية المعلومات والإدارة العامة للمؤسسة. وعلى الرغم من أن قضية أمن تقنية المعلومات كانت دائماً ومنذ الأيام الأولى مصدر قلق، فإن مجال المخاطر هذا أصبح مصدر قلق أكثر من ذلك بكثير في عالم اليوم الذي يحوي كمّاً هائلاً من اتصالات الإنترنت وكذلك الاعتماد المتزايد على إستراتيجيات الحوسبة السحابية. يكون التدقيق الداخلي والإدارة العليا في المؤسسات غالباً هم الأطراف المعنية بالقراءة عن الخروقات الخاصة بأمن تقنية المعلومات التي تحدث في مكان آخر وسؤال كل من المدير التنفيذي للمعلومات (Chief Information Officer (CIO ومدير التدقيق الداخلي (Chief Audit Executive (CAE ومدققي تقنية المعلومات حول المسائل المتعلقة بأمن تقنية المعلومات في المؤسسة.

تعد المخاوف المتعلقة بأمن تقنية المعلومات من بين القضايا الرئيسية والهامة التي تؤثر في كل من الإدارة العامة وإدارة تقنية المعلومات. وللحصول على ضمانات كافية حول امتلاك أمن فعال لتقنية المعلومات، فإن المؤسسة بحاجة إلى تأسيس وبناء بيئة قوية ومدارة بشكل جيد لأمن تقنية المعلومات. وتعد هذه المهمة مسئولية إدارة عمليات تشغيل تقنية المعلومات وإدارة المؤسسة على جميع المستويات. فإدارة تقنية المعلومات تستطيع المساعدة في هذه العملية من خلال تطبيق ضوابط داخلية فعالة وسياسات وإجراءات أمنية قوية، وكذلك من خلال العمل مع جميع المستويات في المؤسسة لخلق بيئة أمنية فعالة.

سوف يركز هذا الفصل على بناء بيئة فعالة لحوكمة أمن تقنية المعلومات وذلك من ثلاثة منظورات: المنظور الأول، هو أن هناك حاجة لوضع بعض المبادئ القوية الخاصة بأمن نظم تقنية المعلومات، مثل المبادئ التي تمت مناقشتها في الفصل الخامس من هذا الكتاب والذي يدور حول الكوبت، أو تطبيق معايير الأيزو المناسبة التي تناولنا الحديث عنها في الفصل السابع أيضاً من هذا الكتاب. إذ يمكن أن تلعب هذه المبادئ دوراً أساسياً في المساعدة على تأسيس بيئة فعالة لأمن تقنية المعلومات.

أما في ما يخص المنظور الثاني، فهناك حاجة ماسة لتأسيس أمن فعال لمحيط تقنية المعلومات، وذلك في أي عملية تقريباً من عمليات التشغيل الخاصة بتقنية المعلومات. فعلى الرغم من أن المخاطر التي كانت تواجه عمليات تشغيل الحاسب التي كانت تتم في مركز مغلق أيام الحاسبات المركزية أقل بكثير من المخاطر التي تواجه عمليات التشغيل اليوم، فإن المخاطر الأمنية تعد أكبر بكثير في البيئات الخاصة بالتجارة الإلكترونية المعتمدة على شبكة الإنترنت. وسنتحدث عن بعض الضوابط الأمنية الخاصة بمحيط تقنية المعلومات التي ينبغي أن تسهم في التحسين من عمليات حوكمة تقنية المعلومات في تلك المجالات.

أما بالنسبة للمنظور الثالث، فسوف نناقش من خلاله أهمية وضع إستراتيجية أمنية فعالة على مستوى المؤسسة. تماماً مثل مدونة قواعد السلوك للموظف التي تضع مجموعة من القواعد الرفيعة المستوى لجميع أصحاب المصلحة في المؤسسة. فالإستراتيجية الفعالة لأمن تقنية المعلومات هي التي تقوم بتأسيس بعض القواعد المتعلقة بأمن تقنية

المعلومات. إذ يمكن للإستراتيجية الأمنية لتقنية المعلومات المُصممة والمُطبقة على نحو جيد أن تسهم في تحسين العديد من الجوانب الخاصة بعمليات التشغيل في المؤسسة. كما ينبغي على إدارة تقنية المعلومات أن تكون على دراية بأفضل أو أجود الممارسات الفعالة في هذا المجال، وأن تقوم باستخدام تلك الممارسات لتأسيس بيئة فعالة لأمن تقنية المعلومات.

مبادئ أمن تقنية المعلومات في المؤسسة: المعايير الأمنية المتفق عليها:

إن العديد من كبار المديرين اليوم على علم بما يعرف بالمبادئ المحاسبية المقبولة قبولاً عاماً (GAAP) General Accepted Accounting Principles سواء كان ذلك من خلال أعمالهم الخاصة أو اتصالاتهم مع المديرين الماليين في المؤسسة أو مع مدققيهم الخارجيين. وعلى الرغم من أنه استُبدل اليوم بتلك المبادئ (GAAP) بمعايير محاسبية دولية، فإنها تعد بمثابة قواعد غير رسمية تستخدم من قبل العديد من المديرين الماليين ومدققيهم الخارجيين لتقييم الممارسات المحاسبية في المؤسسة، ومن ثم القيام بإعداد القوائم المالية الخاصة بها. فهي ليست قواعد محددة على شكل نقاط، إنما هي عبارة عن مجموعة من الممارسات الجيدة والعامة التي استُخدمت من قبل المدققين الخارجيين على مر السنين.

بأسلوب مماثل للمبادئ المحاسبية المقبولة قبولاً عاماً GAAP، قامت العديد من إدارات تقنية المعلومات المؤسسية بتطبيق ما يعرف بمبادئ أمن النظم المقبولة قبولاً عاماً (GASSP) Generally Accepted System Security Principles كمجموعة من أفضل الممارسات لتطوير عمليات ومعايير فعالة في أمن تقنية المعلومات. GASSP هي عبارة عن مجموعة متفق عليها من المبادئ والمعايير والأعراف والآليات المتعلقة بأمن تقنية المعلومات التي يجب أن توظف من قبل الممارسين لقضايا أمن تقنية المعلومات، والتي يجب أن تحققها المخرجات الناتجة عن معالجة المعلومات، والتي يجب أن يقر بها أصحاب المعلومات لضمان أمن المعلومات وأمن نظم تقنية المعلومات الخاصة بهم. تتعلق GASSP بأمن المعلومات المادية والتقنية والإدارية، كما تشتمل على مبادئ أمنية تفصيلية ووظيفية واسعة ومتعارف عليها. تشير GASSP إلى سلسلة من القواعد والإجراءات والممارسات التي تتعلق بتطبيق الممارسات الفعالة لأمن تقنية المعلومات في المؤسسة. ومن المتوقع

أن يتطور هذا المفهوم الخاص بمصطلح GASSP وفقاً للتغيرات السريعة والمستمرة في التقنيات الخاصة بتقنية المعلومات.

تعود أصول هذه المبادئ المقبولة قبولاً عاماً في أمن معلومات النظم GASSP إلى عام ١٩٩٠ عندما قام مجلس البحوث الوطني الأمريكي بإصدار كتاب أحدث تحولاً بارزاً بعنوان "الحاسبات عرضة للمخاطر" ^(١) Computers at Risk (CAR)، وقد ركز هذا الكتاب على أن الولايات المتحدة الأمريكية بحاجة ماسة إلى أن تركز اهتمامها بشكل أفضل على أمن المعلومات. وقد وُجدت GASSP لتكون نتيجة مباشرة لإحدى التوصيات الرئيسية التي جاءت من نشر هذا الكتاب (CAR) وقد دعت تلك التوصية إلى تطوير مجموعة شاملة من المبادئ المقبولة قبولاً عاماً في أمن النظم والتي من شأنها أن تقدم تعريفاً واضحاً للسمات والضمانات والممارسات الأساسية الخاصة بأمن تقنية المعلومات. كما اقترح كتاب CAR استخدام GAAP نموذجاً يُقتدى به في وضع GASSP، كما استشهد أيضاً بالصياغة الخاصة بالقواعد والمعايير المستخدمة من قبل مختبرات ضمان المواصفات ^(٢) Underwriters Laboratories بأنها أمثلة على GASSP في مجالات أخرى.

يعد الاتحاد الدولي لاعتماد أمن نظم المعلومات ^(٣) International Information Systems Security Certification Consortium (ISC) من المنظمات المهنية الأخرى الرائدة في أمن تقنية المعلومات والتي قامت بتطوير GASSP في نسخته الحالية (الإصدار الثاني Version 2.0) والتي تم إطلاقها في عام ١٩٩٣ ^(٤). وكما يدل عليها اسمها، فهي عبارة عن المبادئ المقبولة قبولاً عاماً أو المتعارف عليها، الأمر الذي يعني أنها تستخدم المفاهيم الشائعة الاستخدام في وقتنا الحاضر لتأمين موارد تقنية المعلومات. إن المبادئ التي جاءت في الدراسة الخاصة بمفهوم GASSP ليست جديدة بالنسبة للعاملين في أمن تقنية المعلومات، ولكنها اعتمدت على افتراضات ينبغي تقريباً على كل شخص تطبيقها عند القيام بتطوير أو صيانة نظام أمن تقنية المعلومات. لذا يجب على مدير المؤسسة التي تسعى إلى تعزيز العمليات الأمنية لتكون جزءاً من الحوكمة الفعالة لتقنية المعلومات، أن يكون على دراية بمبادئ GASSP بوصفه معياراً أو أسلوباً لتعزيز الأمن الفعال لتقنية المعلومات.

المبادئ المتعارف عليها في أمن النظم والمقبولة عموماً GASSP:

ترتكز GASSP على ثمانية مبادئ رفيعة المستوى يمكن أن تستخدم من قبل الإدارة وأخصائيي أمن تقنية المعلومات أساساً أو قاعدة ليقوموا ببناء برامجهم المتعلقة بأمن تقنية المعلومات عليها. وتهدف هذه المبادئ لأن تكون بمثابة دليل أمني يمكن استخدامه عند إنشاء نظم أو ممارسات أو سياسات جديدة. فهي لم تُصمم لإعطاء إجابات محددة، بل يجب تطبيقها جملة واحدة وبشكل عملي ومعقول. وفيما يلي توضيح لكل من هذه المبادئ الثمانية الخاصة بمفهوم GASSP.

١. يجب على أمن تقنية المعلومات دعم رسالة المؤسسة: إن الغرض من أمن تقنية المعلومات هو حماية الموارد القيمة في المؤسسة كالمعلومات والمعدات والبرمجيات. فمن خلال اختيار وتطبيق وسائل الحماية المناسبة، يمكن للأمن أن يساعد المؤسسة على تحقيق رسالتها، وذلك من خلال حماية مواردها المادية والمالية وسمعتها ووضعها القانوني وموظفيها وغيرها من الأصول الملموسة وغير الملموسة. وللأسف فإنه يُنظر لأمن تقنية المعلومات في بعض الأحيان على أنه عائق في طريق تحقيق رسالة المؤسسة، وذلك من خلال فرض القواعد والإجراءات المُرهِقَة التي يتم اختيارها بشكل سيئ، على المستخدمين والمديرين والنظم. ونتيجة لذلك فإنه يجب على إدارة تقنية المعلومات أن تكون على علم بأن القواعد والإجراءات الأمنية التي تم اختيارها بعناية لم تُوضع لحماية مصالحهم الخاصة، وإنما وضعت موضع التنفيذ لحماية الأصول الهامة ودعم الرسالة التنظيمية الشاملة للمؤسسة.

ولذلك فالأمن يعد وسيلة للوصول إلى الغاية وليس غاية في حد ذاته. فعلى سبيل المثال، يكون للممارسات أو الإجراءات الأمنية المستخدمة عادةً دور ثانوي في عملية تحقيق الأرباح المؤسسية التي هي الهدف الرئيسي لأي مؤسسة. لكن يجب بعد ذلك أن يكون للأمن دور رئيسي في زيادة قدرة المؤسسة على تحقيق الأرباح. أما في مؤسسات القطاع العام، فيلعب الأمن عادةً دوراً ثانوياً فيما يتعلق بالخدمات التي تقدمها المؤسسة للمواطنين، إلا أنه يتوجب على الأمن فيما بعد أن يلعب دوراً أساسياً في تحسين هذه الخدمات العامة. لذلك فإن المديرين وأخصائيي الأمن بحاجة إلى فهم كلٍّ من الرسالة الشاملة للمؤسسة والكيفية

التي يمكن من خلالها أن يقوم كل نظام من نظم تقنية المعلومات بدعم تلك الرسالة. وبعد أن يتم تحديد أدوار تلك النظم، يمكن الإعلان صراحة عن تلك المتطلبات الأمنية الخاصة برسالة المؤسسة.

٢. أمن تقنية المعلومات جزء لا يتجزأ من الممارسات الإدارية الصحيحة: تكون نظم تقنية المعلومات غالباً من الأصول الهامة التي تدعم رسالة المؤسسة. لذا فحماية تلك الأصول أمر لا يقل أهمية عن حماية الموارد الأخرى، مثل الأموال أو الأصول المادية أو الموظفين. من ناحية أخرى، فإن تضمين الاعتبارات الأمنية في إدارة نظم المعلومات وإدارة نظم تقنية المعلومات لا يستبعد بشكل كامل احتمالية أن يتم الإضرار بهذه الأصول. في النهاية، يجب على الإدارة أن تقرر ما مستوى المخاطر المستعدة لقبولها، مع الأخذ في الحسبان تكلفة الضوابط الأمنية.

كما هو الحال مع غيرها من الموارد، فإن إدارة نظم المعلومات وإدارة نظم تقنية المعلومات قد تتجاوز الحدود التنظيمية. فعندما تكون نظم معلومات ونظم تقنية المعلومات الخاصة بالمؤسسة مرتبطة بنظم خارجية، فإن مسؤوليات الإدارة ستمتد لتتجاوز حدود المؤسسة، وإن كلاً من الإدارة وإدارة تدقيق تقنية المعلومات يجب أن يعرفوا ما مستويات أو أنواع الأمن التي يتم توظيفها على تلك النظم الخارجية، كما يجب أن يسعوا للحصول على ضمانات بأن النظام الخارجي يوفر الأمن الكافي لاحتياجات المؤسسة التابعين لها.

٣. أمن تقنية المعلومات يجب أن يكون فعالاً من حيث التكلفة: يعد هذا الأمر من المبادئ الهامة لحوكمة تقنية المعلومات. وعليه فإنه يجب عمل دراسة للتكاليف والفوائد الخاصة بأمن تقنية المعلومات بعناية، سواء من الناحية المالية أم غير المالية للتأكد من أن تكلفة الضوابط لن تزيد عن الفوائد المتوقعة. فأمن تقنية المعلومات يجب أن يكون ملائماً ومتناسباً مع قيمة ودرجة الاعتماد على نظم تقنية المعلومات وكذلك مع شدة واحتمالية ومدى الضرر المحتمل. كما أن المتطلبات الأمنية تتنوع اعتماداً على النظام المحدد لتقنية المعلومات.

يجب أن يُنظر لأمن تقنية المعلومات على أنه أحد الممارسات الذكية للأعمال. وأن الاستثمار الجيد في التدابير الأمنية للمؤسسة يمكن أن يساعد في التقليل من تكرار وشدة

الخسائر المتعلقة بأمن تقنية المعلومات. فعلى سبيل المثال، قد تقدر المؤسسة أنها تعاني من خسائر سنوية كبيرة في المخزون من خلال المعاملات الاحتيالية التي تتم في نظام تقنية المعلومات الخاص بمراقبة المخزون لديها. فباستخدام التدابير والإجراءات الأمنية المناسبة، كالنظام المطور الخاص بضبط عمليات الوصول للبيانات، قد يسهم بشكل كبير في التقليل من هذه الخسائر. علاوة على ذلك، فإن البرنامج الأمني السليم يمكنه إحباط محاولات القرصنة Hackers والتقليل من تكرار الإصابة بالفيروسات.

للفوائد الأمنية تكاليف مباشرة وغير مباشرة. حيث تشتمل التكاليف المباشرة على شراء وتركيب وإدارة التدابير والإجراءات الأمنية، كبرامج ضبط الوصول إلى البيانات أو النظم المستخدمة لإخماد الحرائق في مرافق المؤسسة. هذا بالإضافة إلى أن استخدام التدابير والإجراءات الأمنية قد يؤثر في بعض الأحيان في أداء النظم وفي معنويات الموظفين وحتى في المتطلبات الخاصة بإعادة التدريب. فكل هذه الأمور يجب أن تؤخذ بعين الاعتبار بالإضافة إلى التكلفة الأساسية الخاصة بالضوابط الأمنية لتقنية المعلومات نفسها. في كثير من الحالات، كما هو الحال بالنسبة لتكاليف إدارة حزمة ضبط الوصول للبيانات، يمكن لهذه التكاليف الإضافية أن تتجاوز التكاليف المبدئية المخصصة للضوابط الأمنية. لذا يجب عدم اختيار الحلول الأمنية إذا كانت تكلفتها من الناحية المالية أو غير المالية أو المباشرة أو غير المباشرة ببساطة أكبر من تكلفة تحمل المشكلة.

٤. لدى أصحاب النظم مسؤوليات أمنية خارج مؤسساتهم: إذا كان للنظام مستخدمون من خارج المؤسسة، فإنه يقع على عاتق أصحاب هذا النظام مسؤولية مشاركة هؤلاء المستخدمين بالمعلومات المناسبة والضرورية المتعلقة بالتدابير الأمنية المستخدمة ومدى النطاق العام لها، الأمر الذي يزيد مستوى الثقة لدى هؤلاء المستخدمين بأن نظامهم آمن بشكل كافٍ. ولا يعني هذا أنه يجب على جميع النظم تحقيق المستوى الأدنى من أمن المعلومات، وإنما يعني أنه يجب على أصحاب النظم إبلاغ عملائهم أو مستخدميهم بطبيعة وآلية أمن المعلومات المستخدمة لديهم.

إن الاختلاف بين المسؤولية والمسئولة المتعلقة بأمن تقنية المعلومات ليس واضحاً دائماً. بشكل عام نستطيع القول إن "المسؤولية" هي مصطلح أوسع يحدد الواجبات والسلوكيات

المتوقعة. إذ يدل مصطلح المسؤولية على الموقف الاستباقي من جانب الطرف المسؤول، وعلى العلاقة السببية بين الطرف المسؤول ونتيجة محددة. في حين يشير مصطلح "المساءلة" بشكل عام إلى قدرة تحمل الأشخاص لمسؤولية أفعالهم. لذلك قد يكون الأشخاص مسؤولين عن أفعالهم دون أن يتعرضوا للمحاسبة القانونية عنها. على سبيل المثال، المستخدم المجهول الهوية الذي يقوم باستخدام أحد النظم يكون مسئولاً أن يتصرف وفقاً للمعايير المقبولة والمتفق عليها، إلا أنه لا يمكن مساءلته إذا قام بأي انتهاك للبيانات أو النظم، إذ لا يمكن تتبع العمل المتسبب في الانتهاك الأمني الذي يقوم به شخص ما.

يدل هذا المفهوم ضمناً على أن الناس والمؤسسات يتشاركون في المسؤوليات والمساءلات المتعلقة بنظم تقنية المعلومات الخاصة بهم. فبالإضافة إلى مشاركة المعلومات المتعلقة بالأمن، يجب على مديري المؤسسات أن يتصرفوا في الوقت المناسب ويتخذوا الإجراءات المناسبة لمنع الخروقات الأمنية والرد عليها لمساعدة الآخرين وحمايتهم من الضرر. فضلاً عن أن اتخاذ مثل هذا الإجراء يجب ألا يُعرض أمن النظم للخطر.

5. المسؤوليات والمساءلات الخاصة بأمن تقنية المعلومات يجب أن تتم بشكل صريح: يجب أن تكون المسؤوليات والمساءلات الأمنية واضحة وصريحة، سواء أكانت تخص أصحاب ومقدمي ومستخدمي نظم تقنية المعلومات أم غيرهم من الأطراف المعنية بأمن نظم تقنية المعلومات. وقد يكون نطاق هذه المسؤوليات داخل المؤسسة أو خارج حدودها. حتى وإن كانت مؤسسة صغيرة فإنه يجب أن تقوم بإعداد الوثائق التي تحدد السياسات الأمنية والمسؤوليات الواضحة لأمن تقنية المعلومات للمؤسسة. على كل حال، فلا يُقصد بهذا المفهوم وجوب مساءلات الفرد عن جميع النظم. فعلى سبيل المثال، لا تسأل العديد من نظم نشر المعلومات عن هوية المستخدم ولا تستخدم أياً من الوسائل التقنية الأخرى لتحديد هويته، ومن ثم لا يمكنها مساءلة المستخدمين.

6. أمن تقنية المعلومات يتطلب نهجاً شاملاً ومتكاملاً: إن توفير أمن فعال لتقنية المعلومات يتطلب استخدام نهج شامل يأخذ بعين الاعتبار مجموعة متنوعة من المجالات الموجودة داخل وخارج مجال أمن تقنية المعلومات، وتمتد طوال دورة حياة نظم المعلومات بالكامل. ولكي تعمل الضوابط الأمنية بفاعلية، فإنها تعتمد غالباً على

التوظيف السليم للضوابط الأخرى، إذ هناك العديد من الاعتمادات المتبادلة فيما بينها. فإذا تم اختيار الضوابط الإدارية والتشغيلية والتقنية بشكل سليم فيمكنها أن تعمل معاً بصورة تعاونية. من ناحية أخرى، فإن عدم فهم المؤسسة للاعتمادات المتبادلة للضوابط الأمنية، قد يُضعف بعضها بعضاً. فعلى سبيل المثال، عدم تلقي التدريب المناسب المتعلق بطريقة وزمن استخدام حزم برامج الكشف عن الفيروسات قد يجعل المستخدمين يطبقون هذه الحزم بشكل خاطئ، ومن ثم يُصبح استخدام تلك الحزم غير فعال. ونتيجة لذلك قد يعتقد المستخدمون خطأً أنه إذا تم فحص النظام لمرة واحدة فقط، فإنه سيكون دائماً خالياً من الفيروسات، ونتيجةً لذلك الاعتقاد الخاطئ ربما تنتشر الفيروسات بشكل غير مقصود. في الواقع، تكون تلك الاعتمادات المتبادلة أكثر تعقيداً ومن الصعب جداً التحقق منها.

تعتمد فاعلية الضوابط الأمنية أيضاً على عوامل مثل إدارة النظم، والقضايا القانونية، وضمان الجودة، والضوابط الداخلية والإدارية. كما يحتاج أمن تقنية المعلومات أيضاً إلى العمل مع الإدارات الأمنية التقليدية في المؤسسة متضمنة وحدات أمن الممتلكات والأفراد. كما يوجد العديد من الاعتمادات المتبادلة الأخرى الهامة التي تكون عادة فريدة بالنسبة لبيئة المؤسسة أو بيئة النظام. لذا يجب على المديرين أن يدركوا كيف يرتبط أمن تقنية المعلومات مع المجالات الأخرى للنظم وكيف يرتبط أيضاً مع إدارة المؤسسة.

٧. يجب إعادة تقييم أمن تقنية المعلومات بشكل دوري: تمتاز نظم تقنية المعلومات والبيئات التي تعمل فيها بأنها متغيرة. أي أن تقنية ومستخدمي النظام، والبيانات والمعلومات داخل النظام، والمخاطر المرتبطة بالنظام، والمتطلبات الأمنية جميعها دائمة التغير. وهناك عدة أنواع من التغيرات التي يمكن أن تؤثر في أمن النظم، تشمل التطورات التقنية، والتغيرات في قيمة أو استخدام المعلومات، وظهور تهديدات جديدة. أضف إلى ذلك، أنه لم يتم اختبار الأمن ولم يكن مكتملاً عند تطبيق النظام. ويتمكن مستخدمو ومشغلو النظام غالباً من اكتشاف أساليب جديدة لتجاوز أو تقويض الأمن، سواء كان ذلك بقصد أم بدون قصد. فالتغيرات التي تطرأ على أحد نظم تقنية المعلومات أو البيئة

التشغيلية الخاصة به يمكن أن تتسبب في إيجاد ثغرات أمنية جديدة. كما أن الالتزام والتقييد الصارم بالإجراءات الأمنية أمرٌ نادر جداً، بل إن هذه الإجراءات تصبح قديمة بمرور الوقت، الأمر الذي يجعل من الضروري إعادة تقييم أمن نظم تقنية المعلومات بشكل دوري.

٨. أمن تقنية المعلومات مُقيد بعوامل اجتماعية: قد تكون قدرة أمن تقنية المعلومات على دعم رسالة المؤسسة محدودة ومقيدة بعوامل مثل القضايا الاجتماعية، فقد يحدث تعارض بين الأمن وخصوصية مكان العمل. فعلى سبيل المثال، يتم تطبيق أمن نظم تقنية المعلومات غالباً من خلال تحديد المستخدمين ومتابعة أعمالهم التي يقومون بها. من ناحية أخرى، تتنوع توقعات الخصوصية كما يمكن أن يتم انتهاكها من خلال بعض التدابير الأمنية. ومع أن الخصوصية تعد قضية اجتماعية في غاية الأهمية، فإنها ليست المسألة الوحيدة المهمة. فتدفع المعلومات، وخاصة بين الحكومة ومواطنيها، تعتبر حالة أخرى قد تحتاج الإجراءات الأمنية فيها إلى بعض التعديلات لدعم الهدف المجتمعي. هذا بالإضافة إلى أن بعض التدابير المستخدمة للتحقق من صلاحيات مستخدمي النظم يمكن اعتبارها اختراقات للخصوصية في بعض البيئات والثقافات.

لذلك يجب أن يتم تحديد الإجراءات الأمنية وتنفيذها في ظل الاعتراف بحقوق الآخرين ومصالحهم المشروعة. وقد يتطلب ذلك تحقيق مزيد من التوازن بين الاحتياجات الأمنية لأصحاب المعلومات والمستخدمين وبين الأهداف المجتمعية. فضلاً عن أن القواعد والتوقعات تتغير إزاء الاستخدام الملائم للضوابط الأمنية. وهذه التغيرات إما أن تزيد أو تقلل من الأمن. وليس بالضرورة أن تكون العلاقة بين المعايير الأمنية والمجتمعية علاقة عدائية. فالأمن يستطيع أن يعزز الوصول إلى البيانات والمعلومات وتدفعها من خلال توفير معلومات أكثر دقة وموثوقية وإتاحة أكبر للنظم. كما يستطيع الأمن أيضاً زيادة الخصوصية الممنوحة للفرد أو المساعدة على تحقيق أهداف مجتمعية أخرى تم وضعها من قبل المجتمع.

تطبيق المبادئ الأمنية في إدارة تقنية المعلومات:

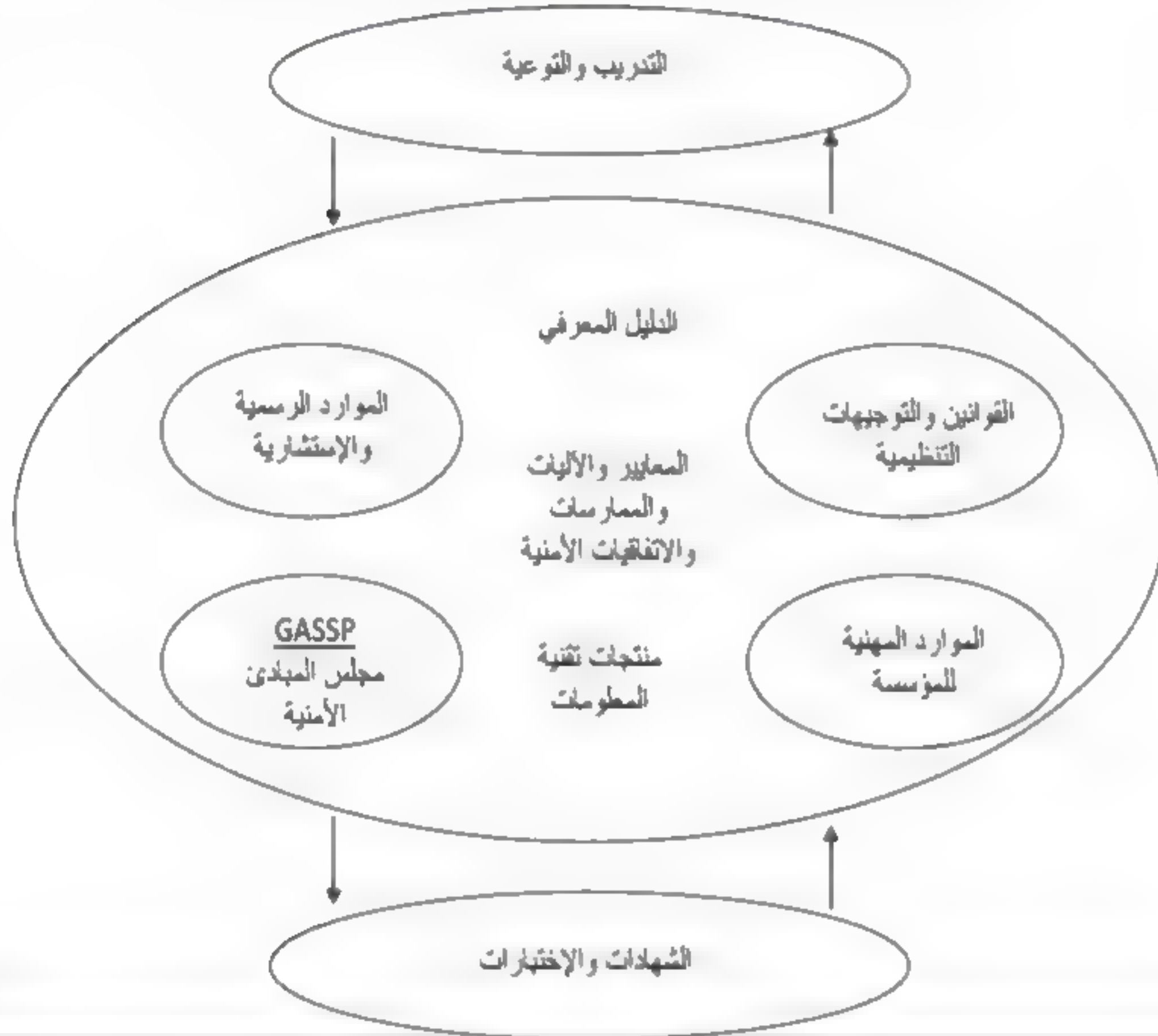
على الرغم من أن مبادئ GASSP الثمانية ليست حتمية، فإنها تلخص الإطار العام الذي يجب أن يكون أساساً للعديد من الجوانب للأمن والحوكمة الرشيدة لتقنية المعلومات. إن تجاوز تلك المبادئ يفرض على وحدة أمن تقنية المعلومات في المؤسسة إعادة التفكير ببعض الممارسات والإجراءات المتبعة حالياً لإعادة تنظيمها بشكل يضمن تبني مبادئ GASSP. يوضح الشكل التوضيحي (١٠-١) الدور الهام الذي تلعبه المبادئ الأمنية الرفيعة المستوى مثل GASSP في المؤسسة، مع إيلاء الاهتمام بمنتجاتها التقنية المثبتة وغيرها من العوامل. وعلى الرغم من وجود العديد من الطرق لتطبيق تلك المبادئ الأمنية، فإنه ينبغي على إدارة تقنية المعلومات ألا تفقد المسار الذي قامت عليه GASSP حيث قامت على بعض المبادئ العريضة والقوية في أمن تقنية المعلومات. وتتناول هذه المبادئ الواسعة الانتشار خصائص سرية، وسلامة، وتوافر المعلومات الخاصة بأمن بتقنية المعلومات. كما توفر تلك المبادئ إرشادات عامة للحوكمة لإنشاء وصيانة أمن المعلومات.

سوف نتحدث عن النقاط الموضحة في الشكل التوضيحي (١٠-١) لكي نصف بإيجاز بعض العناصر الرئيسية الخاصة بمبادئ GASSP وكيفية ارتباط بعضها ببعض وبالبيئة الشاملة لأمن تقنية المعلومات. وقد تختلف أي من هذه المجالات أو النقاط المذكورة حسب المؤسسة وحجمها وموطنها. وسنبداً من مركز الشكل حيث المعايير الأمنية وغيرها من الآليات، صعوداً إلى الدليل المعرفي Body of Knowledge، ثم نسير باتجاه عقارب الساعة حول العوامل الأخرى الضرورية لتشكيل بيئة أمنية فعالة باستخدام مبادئ GASSP.

• **معايير وآليات الأمن:** نواة أي بيئة أمنية فعالة عبارة عن مجموعة من المعايير، والآليات، والممارسات، والاتفاقيات الأمنية القوية التي تخص مؤسسة ما. وهذه هي أنواع القضايا التي تمت مناقشتها خلال فصول هذا الكتاب باعتبارها عمليات رقابية عامة فعالة لحوكمة تقنية المعلومات.

شكل توضيحي (١٠-١)

دور المبادئ رفيعة المستوى لأمن تقنية المعلومات في المؤسسة



• **الدليل المعرفي لمبادئ GASSP:** لقد قمنا هنا بتلخيص مبادئ GASSP، إلا أنه يتوجب على شريحة كبيرة ومختلفة من الأشخاص الذين يعملون في المؤسسة فهم تلك المبادئ العامة، كما يجب عليهم أن يُظهروا التزامهم بفهم وتنفيذ تلك المبادئ بشكل منتظم. الفكرة هنا هي أنه في ظل وجود أي استفسار يتعلق ببعض الممارسات الخاصة بأمن تقنية المعلومات، يتعين على إدارة تقنية المعلومات في المؤسسة في هذه الحالة الرجوع إلى هذه المبادئ العامة لتساعد في تفسير وحل أي قضية من القضايا التي تواجهها.

• **القوانين والتنظيمات التوجيهية:** تخضع كل مؤسسة لمجموعة متنوعة وفي الغالب مختلفة من القوانين واللوائح التنظيمية. وخير مثال على ذلك هنا هو أننا نستطيع أن نلاحظ

الاختلاف الكبير بين قوانين الخصوصية الشخصية من بلد إلى آخر. لذا يجب أن تُفسر مبادئ GASSP دائماً اعتماداً على هذه القوانين والقواعد المختلفة والمتغيرة في بعض الأوقات.

• **الموارد المهنية للمنظمة:** تقوم المنظمات المهنية مثل ISACA و AICPA بانتظام بإصدار مجموعة من الإرشادات والمعايير التي تضيف المزيد من المتطلبات الجديدة على أساليب أمن تقنية المعلومات أو تُغير من تلك الأساليب. لذا يجب على المؤسسة الإلمام بمثل هذه الأمور ثم تقوم بعمل التغييرات المطلوبة على بيئة أمن تقنية المعلومات الخاصة بها بما يتفق مع هذه الإرشادات والمعايير الجديدة.

• **منتجات البنية التحتية والأمنية لتقنية المعلومات:** هناك مجموعة متنوعة وواسعة من تطبيقات ومنتجات البنية التحتية لتقنية المعلومات التي تستطيع أن تساعد في عملية توجيه أو تعديل الأساليب الخاصة بأمن تقنية المعلومات. فبينما لا يجب على المؤسسة أن تقوم بتثبيت المنتجات التي تعاني قصوراً في هذه المبادئ الأمنية، نجد أنه من الضروري أن تكون المؤسسة على علم بأي خصائص جديدة وفريدة للمنتجات التي تم تثبيتها وإجراء التعديلات المناسبة على الممارسات الأخرى لأمن تقنية المعلومات.

• **مجلس المبادئ الأمنية الخاص بمبادئ GASSP:** عندما تقوم المؤسسة باعتماد مبادئ GASSP، فهي بحاجة إلى تكليف بعض الأشخاص الموثوقين ليقوموا بتفسير عمليات تطبيق مبادئ GASSP بصورة سليمة. وقد يأتي الأشخاص المناسبون لهذه المهمة من وحدة أمن تقنية المعلومات، أو من مجموعة ضمان الجودة، أو ممثل عن إحدى الوحدات مثل وحدة التدقيق الداخلي لتقنية المعلومات. وعلى الرغم من أنه قد لا يكون أحد من هذه المجموعة خبيراً بمبادئ GASSP، فإن الفكرة هي تعيين شخص مسئول عن فهم تلك المبادئ يستطيع تفسيرها اعتماداً على الاستفسارات المطروحة ويمكن أن يكون الحكم إذا تطلب الأمر ذلك.

• **الموارد الرسمية والاستشارية:** على الرغم من أنه قد جرت العادة بعدم بيع الخدمات الاستشارية، فإنه يجب على المؤسسة أن تكون على ارتباط وثيق بمنظمات مهنية مثل ISACA و ISC للاطلاع على آخر التعديلات والمواد التفسيرية الأخرى التي طرأت على مبادئ GASSP.

• **التدريب والتوعية:** لن تكون هناك أي قيمة حقيقية تذكر لتطبيق مبادئ GASSP في المؤسسة ما لم يكن هناك تدريب لمجموعة رئيسية من أصحاب المصلحة في هذه المؤسسة على تلك المبادئ. لذا يجب على مطوري النظم على وجه الخصوص أن يفهموا هذه المبادئ جيداً ويستخدموها عند إطلاق التطبيقات الآمنة والفعالة للمؤسسة.

• **الشهادات والاختبارات:** لا يوجد إلى الآن برامج خاصة بشهادات أو اختبارات لمبادئ GASSP. غير أن مثل هذه البرامج قد يتم تطويرها في المستقبل.

ومع أن مبادئ GASSP لم تلق إلى الآن مستوى واسعاً من القبول من قبل المؤسسات في الولايات المتحدة، ففي ظل التغيرات المستمرة والتقدم التكنولوجي العالمي الموجود اليوم، بالإضافة إلى المخاوف المتزايدة لأمن تقنية المعلومات، توفر هذه المبادئ أساساً هاماً أو إطار عمل للنظر في أمن تقنية المعلومات وتقييمه. لذا يجب على كبار المديرين الذين يبحثون عن طرق لإيجاد إجراءات فعالة لأمن وحوكمة تقنية المعلومات، أن ينظروا إلى تلك المبادئ على أنها نقطة بداية لتحقيق الهدف المرجو.

أهمية الإستراتيجية الأمنية الفعالة على مستوى المؤسسة:

من الممكن أن تكون هناك قيمة معتبرة نتيجة تبني مجموعة عريضة من المبادئ الأمنية مثل مبادئ GASSP، إلا أن المؤسسة بحاجة أيضاً إلى تبني وتطبيق إستراتيجية شاملة لأمن تقنية المعلومات. إن الأمن في عالم اليوم الإلكتروني والمرتكز على تقنية المعلومات يشتمل على هياكل معقدة وتقنيات تظهر وتتطور بشكل مستمر. ولكي نضمن أن المؤسسة قد قامت بإنشاء مستويات مناسبة من أمن تقنية المعلومات، ينبغي عليها أن تفكر في استخدام نموذج أمني من أعلى لأسفل Top-Down لتحديد وتقييم أصولها الأمنية. فباستخدام مثل هذا النهج الأمني من أعلى لأسفل، تستطيع الإدارة أن تدرك بشكل أفضل مدى خطورة القضايا الخاصة بأمن تقنية المعلومات، ومن ثم الشروع بتطبيق العمليات التي تتبلور في الأسفل والموجودة لدى فريق عمليات التشغيل. وهذا يختلف عن النهج الذي يتبع نهجاً من أسفل إلى أعلى Bottom Up، حيث يقوم فريق تشغيلي أقل درجة ببدء العملية ومن ثم يقوم بنشر نتائجه صعوداً نحو الإدارة على شكل توصيات للسياسة المقترحة.

يقدم الشكل التوضيحي (٢-١٠) توضيحاً بسيطاً لمفهوم النموذج الأمني من أعلى إلى أسفل Top-Down. وستوضح الفقرات التالية عناصر هذا المفهوم بمزيد من التفصيل. وعليه فإنه يجب تطبيق البنية التحتية لأمن تقنية المعلومات بشكل متساوٍ على الوصلات الشبكية الموجودة مسبقاً والوصلات الجديدة للمبادرة، بعد ذلك يجب حماية الشبكة الخاصة بالمنظمة بناءً على المخاطر التي تمثلها تلك الشبكة للمنظمة.

المستوى الأعلى من النموذج الموجود في الشكل التوضيحي (٢-١٠) يدعو إلى سياسات أمنية فعالة. ومع أن الأمر قد يبدو في بعض الأحيان وكأنه واضح للغاية، فإنه ينبغي على المدير الأول الذي يقوم بمراجعة الضوابط الموجودة في البيئة الأمنية لتقنية المعلومات أن يقوم بداية بتعهد فهم السياسات الأمنية الحالية لتقنية المعلومات في المؤسسة. وعلى الرغم من أن هذه السياسات تكون في العادة رفيعة المستوى، فإن أي مجموعة سياسات كهذه يجب أن تغطي الجوانب الأمنية كافة لتقنية المعلومات. وربما يكفي أن نذكر أن السياسات الأمنية لتقنية المعلومات في المؤسسة سوف تستند إلى المبادئ الخاصة بمعايير الأيزو التي تمت مناقشتها في الفصل السابع من هذا الكتاب وكذلك مبادئ كوبت التي تمت مناقشتها في الفصل الخامس من هذا الكتاب.

ويجب أن تكون هذه الإستراتيجيات الأمنية مدعومة بمعايير أمنية تفصيلية تشمل عمليات تنفيذ مراقبة النظم، وتهيئة النظام للعمل كخادم تطبيقات أو خادم ويب، أو تهيئة الجدران النارية لفصل النظم ووضعها في مناطق محددة. كما يجب أن تكون هذه المعايير خاصة بكل من التطبيقات ونظم التشغيل، وأن تكون مفصلةً على نحو كافٍ لتتمكن المستخدم صاحب المعرفة من القيام بتنفيذ أبرز النشاطات الموجودة في أحد المعايير أو تمكنه من تهيئة النظام أو التطبيق. وأخيراً يجب على هذه المعايير أن تحدد الخطوات التي يجب اتخاذها، مثل الموافقة، في حال كان الإخلال بهذه المعايير أمراً ضرورياً.

علينا أن نفكر في العمليات التشغيلية لأمن تقنية المعلومات باعتبارها سلسلة من مناطق الثقة. بمعنى أنه يجب على عمليات التشغيل الخاصة بتقنية المعلومات أن تقوم بتحديد وتصنيف جميع الوصلات والنظم الحالية داخل الأماكن المنطقية المتعلقة بالأمن. أحد العناصر الرئيسية في هذا التصنيف الأمني هو الوصول إلى الإنترنت والوصلات الشبكية

الأخرى مثل نظم الدعم الخاصة بالبائعين. وفيما يلي أربعة تصنيفات ممكنة لمثل هذه النظم المتداخلة:

شكل توضيحي (١٠-٢)

مفهوم نموذج أمن تقنية المعلومات من أعلى لأسفل



١- **النظم والعمليات الموثوقة:** هي النظم التي تخضع مباشرة لسيطرة إدارة تقنية المعلومات. فمن المحتمل أن يحتاج المستخدمون والنظم إلى صلاحيات الوصول الكامل لجميع النظم الداخلية لتقنية المعلومات بشكل أساسي.

٢- **نظم شبه موثوقة:** هي النظم الخاصة بدعم الموردين وبعض شركاء الأعمال. والتي تحتاج إلى صلاحيات وصول موثوقة لحماية النظم المكشوفة التي لا تكون متاحة لعامة الناس.

٣- **نظم غير موثوقة:** هي غالباً النظم والعمليات المرتبطة بالعميل والتي تتطلب حقوق وصول موثوقة لمصادر معلومات محددة. هذا بالإضافة إلى النظم المكشوفة والمتاحة لعامة الناس.

٤- **النظم العدائية وتهديدات العملية:** حقوق وصول مقيدة ومحددة جداً فقط هي التي يُسمح بها للوصول إلى مثل هذه النظم. وينبغي الكشف عن محاولات الوصول غير المصرح بها في الوقت الحقيقي.

عقب هذه التصنيفات، لا بد من إعادة النظر في جميع المستويات الخاصة بروابط أو علاقات تقنية المعلومات مثل دعم الموردين والعملاء والشركات الفرعية التابعة وشركاء الأعمال ووضعها على مستوى من الثقة وفقاً لأنواع الضوابط التي يمكن المحافظة عليها. فضلاً عن أن تحديد كل رابط في منظمة كبيرة يمكن أن يكون في أحسن الأحوال أمراً صعباً. من الوسائل الفعالة لعمل تصنيف كهذا هو القيام بعقد ورشة عمل يشارك فيها مجموعة كبيرة من أعضاء طاقم العمل ذوي المعرفة والاطلاع المدركين للمفاهيم المرتبطة بأعمال المؤسسة والمشاريع وعلى علم بالمشاريع الأخرى داخل المؤسسة وبعمليات التشغيل الخاصة بتقنية المعلومات فيها. ومع أنه من غير المرجح تحديد الروابط كافة في ورشة عمل واحدة، فإن هذا النوع من الممارسة قد يساعد على تحديد أغلبية الروابط، ويساعد أيضاً على تحديد أعضاء طاقم العمل الآخرين في المؤسسة الذين قد يكونون مسؤولين عن تحديد تلك الروابط وغيرها.

لا بد من توثيق هذه الروابط أو العلاقات وكذلك بروتوكولات الاتصالات الشبكية الخاصة بها واستخدامها لوضع ضوابط تفصيلية للسماح بالوصول من المواقع المناسبة المقصودة وإليها. ونتيجة لذلك فإنه ينبغي على المؤسسة الفصل بين الأجزاء المختلفة من شبكتها إلى عدة مناطق ثقة.

إن عملية فصل وتصنيف النظم والعمليات تعمل على فصل النظم اعتماداً على فئات محددة من الثقة. لذا يجب أن يكون هناك دائماً لدى الشبكة الداخلية لتقنية المعلومات في المؤسسة الجزء الشبكي الخاصة بها، مشتملاً على خادم الويب، وخادم البريد الإلكتروني، وخادم اسم النطاق وغيرها من الخوادم الأخرى التي يجب أن يتم تصنيفها إلى مناطق ثقة وأن يتم تقسيمها أو تجزئتها بشكل مناسب. قد يؤدي هذا إلى تجزئة كل خدمة من هذه الخدمات ووضعها في مناطق منفصلة أو قد يؤدي إلى تنفيذ عدد من هذه الخدمات في منطقة واحدة. وسيعتمد التصميم النهائي للهيكل الأمني المحيط على هذا التصنيف الخاص

بالنظم والخدمات، غير أن تصميم تلك المناطق والتصنيفات يعد أحد العناصر الحساسة للأمن المحيط بتقنية المعلومات.

تخطيط استمرارية تقنية المعلومات:

على مر السنين وخاصة في زمن استخدام الحواسيب المركزية القديمة، كان مدققو تقنية المعلومات في المؤسسة يقومون غالباً بإثارة العديد من القضايا التي تتعلق بمخاطر فقدان المؤسسة لقسم كبير من مواردها الخاصة بتقنية المعلومات نتيجة وقوع أحداث كارثية. الأمر الذي كان مصدر قلق كبير، وخصوصاً في الأيام الأولى لظهور تقنية المعلومات عندما كانت معظم العمليات التشغيلية للنظم تعتمد على النظم المركزية، حيث كان هناك القليل من وصلات الاتصالات لربط الموارد الخاصة بتقنية المعلومات، وقد كان يتم في هذه النظم المركزية القديمة تثبيت جميع التركيبات المطلوبة تقريباً من قبل البائع، إذ إن تركيب نظام جديد كان يستلزم جهوداً ضخمة.

وقد أدركت الإدارة العليا لاحقاً مخاطر تعطل تلك النظم، واستجابة لتلك المخاوف قامت أقسام تقنية المعلومات بتطوير إستراتيجيات بديلة للمعالجة. إن هذا التطوير الذي حدث في النظام والذي أصبح يعرف باسم التخطيط للتعافي من الكوارث الخاصة بتقنية المعلومات، وفيه ستقوم المؤسسة غالباً بعمل الترتيبات اللازمة لتجهيز الموقع البديل الخاص بالمعالجة لتغطية مخاطر تعطل النظام المركزي. ونظراً لأن تنفيذ مثل هذه الخطط قد يكون مكلفاً، فإن مديري التدقيق الداخلي وغيرهم من المديرين في كثير من الأحيان كانت لديهم صعوبة في الترويج وتنبيه الإدارة العليا من تلك المخاطر. يسترجع مؤلف هذا الكتاب ذكرياته عندما كان يدير إحدى عمليات تدقيق تقنية المعلومات الخاصة بتخطيط التعافي من الكوارث لإحدى الشركات التي أصبحت فيما بعد من أكبر الشركات الأمريكية في مطلع التسعينيات من القرن الماضي، حيث كان واحد من المراكز الرئيسية للبيانات الخاصة بالشركة يقع بالقرب من أحد المطارات المزدهم بحركات الطائرات - مع وجود مخاطرة تتعلق بوقوع حوادث طيران - حيث لم تكن هناك أي خطة فعالة جاهزة للتعافي من الكوارث. وعندما قام قسم التدقيق الداخلي وللمرة الأولى بإثارة المخاوف المتعلقة بعدم وجود خطة فعالة لاسترجاع تقنية المعلومات، قام وقتها الرئيس التنفيذي للمعلومات CIO

بتجاهل هذه المخاوف قائلاً إن مثل هذه الكوارث لا يمكن أن تحدث أبداً. وفي النهاية قام هذا المؤلف مع إدارة التدقيق الداخلي بإثارة تلك المخاوف في أحد الاجتماعات مع لجنة التدقيق لتهيئة الشركة لإطلاق مثل هذه الجهود الخاصة بالتخطيط لمواجهة الكوارث.

خلال الفترة من ثمانينيات وحتى مطلع تسعينيات القرن الماضي، كان الحل الشائع للتعافي من الكوارث المتعلقة بتقنية المعلومات بالنسبة للمؤسسات الكبيرة هو التنسيق مع أحد المرافق البعيدة المخصصة لمعالجة بيانات التعافي من الكوارث لإجراء المعالجات الطارئة. وقد تم تخزين نسخ احتياطية للملفات والبرامج الرئيسية في أماكن خارج موقع العمل الحالي. مع وجود خطط تدعو موظفي تقنية المعلومات إلى التحول لاستخدام تلك المرافق البديلة في حال وقوع الكوارث. اعتقد المهنيون أن كوارث تقنية المعلومات هي فقط الحرائق والفيضانات أو بعض أحوال الطقس السيئة الأخرى. في تلك الأيام الأولى لنظم الحاسبات المركزية القديمة، كانت الشركات تستخدم في بعض الأحيان ما يبدو لنا اليوم وكأنها طرق غريبة لتطوير خططها الخاصة بالتعافي من كوارث تقنية المعلومات. فقد كانت هذه الطرق تقوم على توقيع "اتفاقيات تبادلية" مع مواقع قريبة منها ولديها موارد تقنية مماثلة لمواردها بحيث يمكن لكل منهما أن ينتقل إلى موقع آخر للمعالجة في حال وقع طارئ ما عند أي طرف من الطرفين. إن توقيع اتفاقية تبادلية بين اثنين من المديرين التنفيذيين للمعلومات CIOs يبدو أمراً جيداً من الناحية النظرية، إلا أنها في الواقع لن تقدم أكثر من مجرد مساعدة إنسانية بشكل أساسي. فربما يكون هذا الموقع القريب الذي تم إبرام اتفاقية تبادلية مع القائم عليه خارج نطاق الخدمة أيضاً للسبب نفسه من الكوارث الطبيعية المتعلقة بالطقس، أو ربما لن يهتم بأي طرف آخر يقوم بتشغيل النظم الخاصة به في فترات خارج وريديات العمل. وكعائق أخير، فإن المستشار القانوني للشركة قد يكون لديه مجموعة من الأسباب ليقول لا للاتفاقية التبادلية.

في السابق، حيث كان يتم وضع نظم الحاسبات المركزية في مرافق بالأدوار العليا وكانت هناك مساحة للكوابل وغيرها من المعدات الأخرى الموضوعة في الطابق نفسه، وكان هناك عدد محدود من الموردين (مثل IBM، Amdahl, Univac، وقليل غيرهم) هم فقط من يقومون بتركيب وإعداد معظم النظم الخاصة بالحاسبات المركزية تقريباً. لذا فإن عملية

الانتقال إلى نظام بديل في الحالات الطارئة كانت تشكل تحدياً كبيراً. في الحقيقة، إن القيام بهذه العملية اليوم أصبح أسهل بكثير، إذ تكون معدات الحاسب في العادة جاهزة للعمل بدلاً من تلك التي تحتاج إلى تصنيع وتهيئة مخصصة، كما كان شائعاً في الماضي.

لم تكن الخطط الأولى للتعافي من الكوارث دقيقة بدرجة كبيرة. إلا أنه سرعان ما ظهرت مجموعة من بائعي أدوات التعافي من الكوارث الذين لديهم مواقع لنظم الحاسب مجهزة بالكامل والتي تكون متوقفة عن العمل (أو ما كان يسمى بالمواقع "الساخنة" "hot" Sites) لتعمل بصفة مرفق احتياطي في حالة الطوارئ. في تلك الأيام الخاصة بالمرافق المركزية لتقنية المعلومات، كانت الشركات تتعاقد غالباً لاستخدام تلك المواقع "الساخنة" مرافق لها للتعافي من الكوارث، وإجراء الاختبارات الدورية، والاحتفاظ هناك بنسخ احتياطية من الملفات الرئيسية لذا كان على إدارة تقنية المعلومات إعادة التفكير في إستراتيجياتها.

أما في عصرنا الحالي الذي يتميز بالبيئة الافتراضية للتخزين في نظام الخادم-العميل والتطبيقات القائمة على شبكة الإنترنت (تطبيقات الويب) فإن المؤسسة أصبحت تواجه مجموعة جديدة من المخاطر المحيطة بأصول تقنية المعلومات الخاصة بها. فمن الطبيعي ألا يكون هناك جهاز مركزي واحد للتعامل مع التطبيقات الآلية الكبيرة، وإنما يوجد مجموعة واسعة من أجهزة الحاسب المكتبية والخوادم والتسهيلات السحابية وغيرها من النظم المتصلة عادة من خلال وسائل اتصال بالغة التعقيد، وشبكات لإدارة التخزين، وروابط مع الإنترنت. إن المؤسسات لا تضع كافة موارد تقنية المعلومات الخاصة بها تقريباً في مركز بيانات واحد (أو أكثر)، فالإدارة مهتمة بالإبقاء على مرافق تقنية المعلومات الخاصة بها تعمل على أكمل وجه أكثر من قلقها بشأن المخاطر المتعلقة بفقدان أحد مرافق نظم الحاسب المركزية. إن المبدأ الأساسي للتخطيط من أجل التعافي من كوارث تقنية المعلومات كان يعتمد على امتلاك عمليات معمول بها لاستئناف عمليات التشغيل في حال حدثت كارثة ما، يمكن أن تتسبب في تعطيل مركز الحاسب. إن هذا النهج القديم للتعافي من الكوارث لم يعد صالحاً اليوم. فالمؤسسة بحاجة للتخطيط لاستمرارية العمليات التشغيلية لأعمالها في حال التعرض لأحداث غير متوقعة.

فمع وجود نظم الخادم والنظم القائمة على الإنترنت اليوم، نجد أن اللغة والأساليب الإستراتيجية الخاصة بتخطيط استمرارية الأعمال والتعافي من كوارث تقنية المعلومات قد تغيرت. لذا يتعين على المهنيين الآن التفكير في أهمية وجود خطة لاستمرارية الأعمال Business Continuity Plan (BCP) والتي تتكون من الإجراءات والعمليات الضرورية التي يجب اتباعها لاستعادة كل العمليات التشغيلية للأعمال. إن النهج والمطلب الجديد هو وضع خطة لاستمرارية الأعمال BCP بدلاً من وضع خطة للتعافي من الكوارث التي كانت موجودة في السابق. فالمستخدم الذي يقوم باستخدام أحد النظم الخاصة بمعالجة طلبات الشراء عبر الإنترنت تكون درجة اهتمامه بحالة الخادم فيما إذا كان يعمل أو لا أقل من اهتمامه بطلب العميل الذي تم تسليمه عبر موقع الإنترنت فيما إن كان قد تمت معالجته بشكل سليم وفعال أم لا. لذا يجب استعادة وتشغيل التطبيق بشكل سريع وفعال قدر الإمكان، إلا أنه يبقى الهدف الرئيسي وهو دعم واستعادة عمليات الأعمال.

خطط استمرارية الأعمال وحوكمة تقنية المعلومات:

لا يزال بعض مديري تقنية المعلومات ينظرون إلى المخاطر والتعافي من الكوارث من منظور الخطة التقليدية القديمة للتعافي من الكوارث، على الرغم من أن تلك الخطط كانت تعتمد على الحاسبات المركزية القديمة والتي كانت موجودة قبل ظهور الإنترنت بزمان بعيد. في الأيام الأولى لتقنية المعلومات كان هناك تركيز كبير على مسألة التخطيط للتعافي من الكوارث - أي استعادة نظم أجهزة الحاسب والتطبيقات وملفات البيانات الخاصة بتقنية المعلومات - أما استرجاع العمليات الأساسية للأعمال فلم تُعط الدرجة نفسها من الاهتمام. وعلى الرغم من أن التعافي من كوارث تقنية المعلومات لا يزال من الأمور الهامة، إلا أن الإجراءات والممارسات الفعالة التي كانت مستخدمة سابقاً للتعافي من كوارث تقنية المعلومات تكون غالباً ذات قيمة محدودة في ظل عالم اليوم المتصل بالإنترنت، والنظم القائمة على الحوسبة السحابية الموجودة حالياً. ولكي تقوم المؤسسة بدعم عمليات حوكمة تقنية المعلومات الخاصة بها يجب أن تقوم بتثبيت وتنفيذ خطة شاملة قوية لاستمرارية الأعمال BCP تشمل كلاً من استرجاع النظم وعمليات الأعمال الخاصة بها.

بالنسبة لبعض المهنيين، فإن هذه المصطلحات يكتنفها بعض الغموض. فعند البحث في الويب سواء عن "التعافي من كوارث تقنية المعلومات IT disaster recovery" أو "خطة الاستمرارية Continuity Planning" سوف يقدم هذا البحث خليطاً من المراجع المتباينة لكلا المفهومين، متجاهلاً ما نعتبره فروقاً جوهرية بين هذين المجالين. فمعظم هذه المراجع، على الرغم من أسمائها، فهي تركز على التخطيط التقليدي للتعافي من كوارث تقنية المعلومات بدلاً من العمليات الأكثر عمومية والخاصة بخطة استمرارية الأعمال BCP. وفي مثال على هذا اللبس، قامت إحدى المنظمات المهنية ذات مرة بإطلاق اسم معهد التعافي من الكوارث Disaster Recovery Institute (DRI) على معهد إدارة الطوارئ^(٤) Institute for Contingency Management وهو الاسم الذي يعرف به حالياً.

ينبغي على كل مؤسسة أن تمتلك خطة فعالة ومعمولاً بها لاستمرارية الأعمال BCP بصرف النظر عن حجم العمليات التشغيلية أو مدى أهمية موارد تقنية المعلومات الخاصة بها. مع تركيز هذه الخطة على الأشخاص والمرافق المادية وغيرها من الموارد، فإن إطلاق خطة فعالة لاستمرارية الأعمال BCP يتطلب مشاركة طيف عريض من مديري المؤسسة وغيرهم من العاملين. من ناحية أخرى تمثل موارد تقنية المعلومات أحد العناصر الأساسية في خطة استمرارية الأعمال BCP، ولهذا السبب يجب على إدارة المؤسسة أن تدرك وتلعب دوراً أساسياً في ترسيخ خطة استمرارية الأعمال BCP في المؤسسة.

وتمتد الخطة الفعالة لاستمرارية الأعمال BCP إلى ما هو أبعد من تقنية المعلومات لتشمل استعادة واستئناف جميع العمليات التشغيلية في المؤسسة والحفاظ عليها. وعلى الرغم من أن استعادة نظم تقنية المعلومات والبيانات الإلكترونية يعد أمراً هاماً، فإن استرجاع تلك النظم والبيانات لن يكون كافياً دائماً لاستعادة عمليات التشغيل الخاصة بالأعمال. فهناك العديد من الجوانب المتعلقة باستمرارية الأعمال مثل وضع خطة الاستجابة في حال حدوث فيضانات غير متوقعة أثناء عملية استخراج المعادن. على كل حال فإن الحديث في هذا الفصل سيكون عن العمليات التشغيلية للأعمال مع دعم مكثف للعمليات التشغيلية لتقنية المعلومات.

وتشتمل خطة استمرارية الأعمال BCP في المؤسسة على تحديد أولويات أهداف الأعمال وعمليات التشغيل الحرجة ، والتي تعد من الأمور الأساسية لعملية التعافي. لذلك لابد من هيكلة العمليات ضمن إطار عمل على مستوى المؤسسة يأخذ بعين الاعتبار جميع العمليات الهامة ووحدات الأعمال والإدارات والنظم المطلوبة للاستجابة للحلول الخاصة بالخلل والتعافي التي يجب تطبيقها. كما يجب أن يشتمل هذا الإطار على خطة قصيرة وطويلة المدى لعمليات التشغيل الخاصة بالاسترجاع، فبدون العمليات الخاصة بخطة استمرارية الأعمال BCP على مستوى المؤسسة التي تأخذ بعين الاعتبار جميع عناصر الأعمال الحساسة؛ ربما يجعل المؤسسة غير قادرة على استئناف الخدمات التي تقدم للعملاء وغيرها من عمليات التشغيل عند مستويات مقبولة. ومع أن العديد من مؤسسات اليوم تفتقر غالباً إلى وجود خطط كهذه، فإنه يجب على الإدارة أن تقوم بتحديد أولويات الأهداف الخاصة بأعمالها وعمليات التشغيل الحساسة لديها والتي تعد من الأمور الأساسية لبقاء المؤسسة، وذلك على اعتبار أن استعادة جميع وحدات الأعمال قد لا يكون ممكناً بسبب التكلفة، وخدمات الإمداد أو التجهيزات، وظروف أخرى غير متوقعة.

كما يجب أن تشتمل خطة استمرارية الأعمال BCP الفعالة على تحديث منتظم لتلك الخطة بناء على عمليات الأعمال وتوصيات التدقيق والدروس المستفادة من عملية الاختبار. وتشتمل التغيرات في عمليات الأعمال على التطورات التقنية التي تسمح بمعالجة أسرع وأكثر كفاءة، والتي من خلالها يتم تقليل الفترات المقبولة لاسترجاع العملية الخاصة بالأعمال. واستجابة للمطالب التنافسية ورغبات العملاء، فإن العديد من المؤسسات تقترب من فترات أقل للتعافي وتصميم حلول تقنية للتعافي داخل عمليات الأعمال. هذه التطورات التقنية تشدد على أهمية صيانة خطة استمرارية الأعمال BCP على مستوى المؤسسة والحفاظ عليها.

وفضلاً عن أنه قد يوجد العديد من الاختلافات في عمليات التشغيل الخاصة بالأعمال المؤسسية، والعديد من الاختلافات التي تحتاج المؤسسة إلى أن تقوم بها من أجل تحقيق الاستمرارية في حالة وقوع بعض الحوادث أو الكوارث غير المتوقعة؛ فإنه من الصعب وضع وصف تفصيلي للمعايير الخاصة بخطة استمرارية الأعمال BCP. ولتطبيق خطة لاستمرارية

الأعمال BCP، يجب على إدارة المؤسسة أن تأخذ بعين الاعتبار الإرشادات المتعلقة باستمرارية الأعمال التي تم تطويرها بواسطة منظمات مهنية مختلفة كالجمعية الوطنية الأمريكية للحماية من الحريق (National Fire Protection Association (NFPA، التي تم تطويرها من خلال بائعي الحاسبات كشركة أوراكل Oracle وإتش بي HP، أو التي تم تطويرها من خلال منظمات المعايير الوطنية الأخرى. ولعل أفضل المواد الخاصة بأفضل الممارسات المتبعة لاستمرارية الأعمال وأكثرها شهرة، هي التي صدرت عن الهيئة البريطانية الوطنية للمعايير (BSI) www.bsi.gov.uk ومعهد استمرارية الأعمال التابع لها الذي يقوم بنشر إرشادات حول بعض الممارسات الجيدة. هذه المعايير مشابهة لمعايير الأيزو ISO التي تمت مناقشتها في الفصل السابع من هذا الكتاب. ويوضح الشكل التوضيحي (١٠-٣) نظرة عامة حول دورة حياة خطة استمرارية الأعمال BCP وفقاً للمعيار البريطاني BS 25999.

لقد قمنا بوصف هذا النهج الخاص بخطة استمرارية الأعمال BCP على أنها عملية حلقيّة ومستمرة لدورة الحياة، في وسط هذه العملية يوجد ما يعرف بإدارة برنامج خطة استمرارية الأعمال BCP وفي خطوة أولى لإصدار خطة فعالة لاستمرارية الأعمال، يجب على المدير المسؤول في المؤسسة أن يتحمل مسؤولية تعريف وإدارة البرنامج الخاص بوضع خطة استمرارية الأعمال BCP. لقد كانت المؤسسات على مر التاريخ تنظر إلى قسم تقنية المعلومات التابع لها وتفترض أن العاملين بهذا القسم سيقومون بإدارة العمليات التشغيلية الخاصة بخطة استمرارية الأعمال BCP باعتبار أنه الفريق المسؤول عن خطة التعافي من كوارث تقنية المعلومات وعمليات النسخ الاحتياطي للملفات والاختبارات الدورية لهذه الخطة. فضلاً عن أنه في الغالب توجد عمليات ومهام أخرى تخص الاستمرارية تذهب إلى ما هو أبعد من مجرد تقنية المعلومات، كما أن هناك آخرين في المؤسسة ربما يكونون هم الأطراف الأكثر ملاءمة للاضطلاع بمسؤولية هذا البرنامج على مستوى المؤسسة.

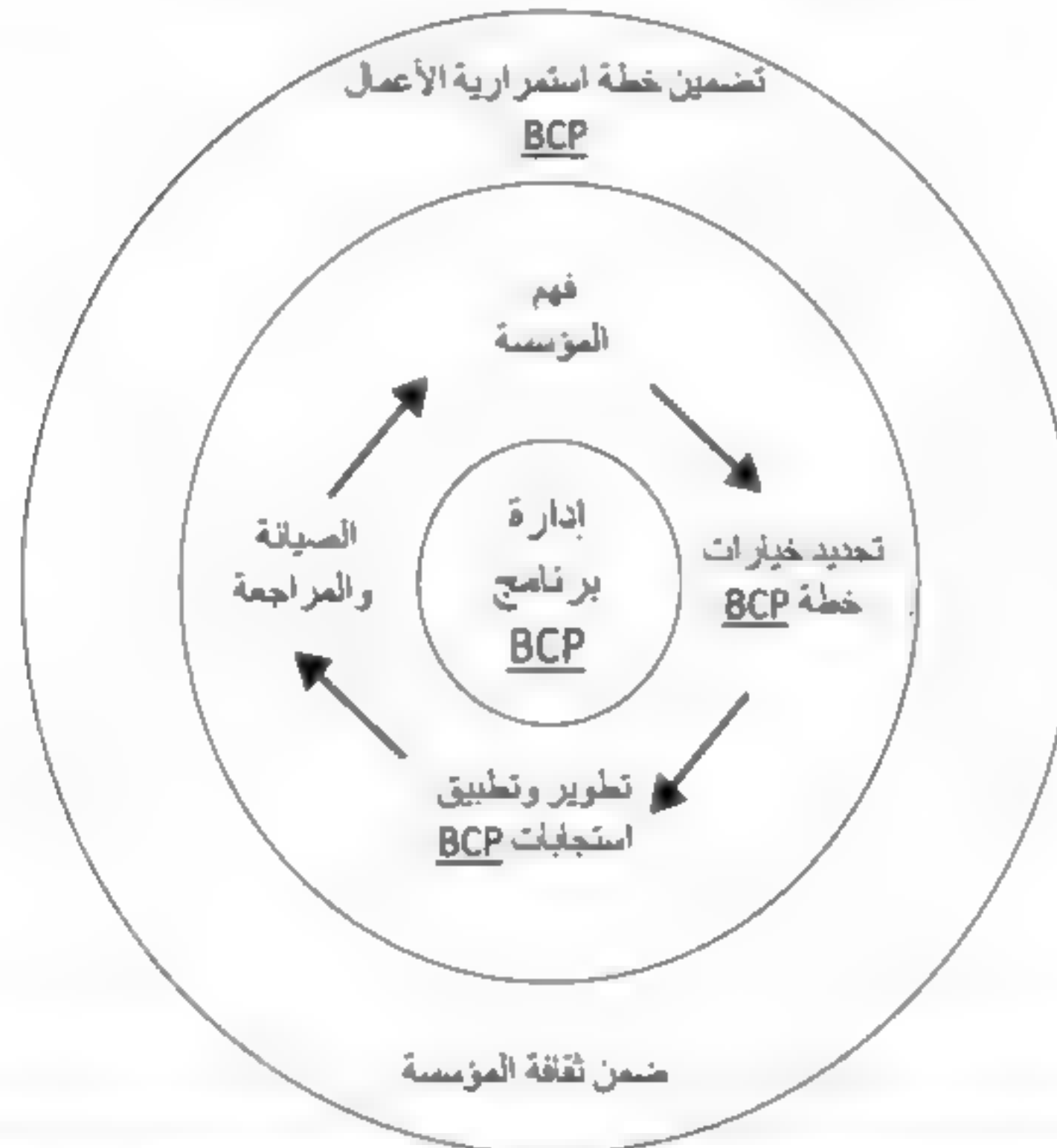
أما في المؤسسات التي يوجد بها وحدة لإدارة المخاطر، يكون المدير التنفيذي للمخاطر عادة هو الشخص الأنسب لتحمل مسؤولية برنامج إعداد خطة استمرارية الأعمال BCP. لكن في حالات أخرى، فإن المدير التنفيذي للمعلومات CIO يمكن أن يتحمل كامل المسؤولية، أو قد يتم إسناد المهمة هنا إلى إدارة ضمان الجودة في المؤسسة. وتعد

خطة استمرارية الأعمال BCP أحد العناصر الهامة للغاية في حوكمة تقنية المعلومات في المؤسسة. وفي جميع الحالات فإنه ينبغي على لجنة التدقيق أن تقوم بمراجعة إستراتيجية خطة استمرارية الأعمال BCP هذه والموافقة عليها.

أضف إلى ذلك أن المؤسسة تحتاج إلى وضع سياسة رفيعة المستوى لتحديد نطاق وأهداف خطط استمرارية الأعمال BCPs الخاصة بها. فمن السهل على المدير الأول أن يصرح بأن خطة استمرارية الأعمال BCP لدى المؤسسة ستغطي كل شيء، غير أن هناك حاجة لمحددات رفيعة المستوى تتعلق بنطاق الخطة. وعلى الرغم من أن تصريحات كهذه قد تبدو رائعة ومثيرة للإعجاب، فإنه قد يكون هناك منتجات أو خدمات معينة لا تحتاج إلى أن تكون في أي مستوى من المستويات العليا في خطط استمرارية الأعمال BCP.

شكل توضيحي (٣-١٠)

دورة حياة خطة استمرارية الأعمال BCP



لابد من تأسيس فريق يعمل تحت إدارة الوحدة المؤسسية التي أسندت إليها مسؤولية إعداد خطة استمرارية الأعمال BCP الخاصة بالمؤسسة. مهمة هذا الفريق تطوير سياسة استمرارية الأعمال للمؤسسة. بحيث تشمل هذه السياسة على ما يلي:

- مراجعة أي مواد حالية متعلقة بالتخطيط لاستمرارية الأعمال في المؤسسة مثل الخطط الموجودة للتعافي من كوارث تقنية المعلومات أو خطط الطوارئ المتعلقة بالأحوال الجوية. وذلك لتحديد مدى ملاءمة الإجراءات الخاصة بخطة استمرارية الأعمال BCP الخاصة بها.

- تحديد أي من إرشادات الممارسات الجيدة أو التنظيمات أو التشريعات التي يجب تضمينها في أي خطة لإدارة استمرارية الأعمال BCM.

- إجراء تقييم رفيع المستوى للمخاطر المتعلقة بخطة استمرارية الأعمال BCP، بمعنى، تحديد جميع النظم الرئيسية وخطوط الإنتاج ووحدات الأعمال وغيرها من الإدارات التي تتطلب أولويات عليا لاستمرارية أعمالها

- تطوير سياسة المؤسسة لاستمرارية الأعمال ومناقشة فرضياتها للحصول على موافقة الإدارة العليا ولجنة التدقيق.

- نشر السياسة التي تمت الموافقة عليها لخطة استمرارية الأعمال BCP على أنها دليل رفيع المستوى لإطلاق البرنامج الشامل لاستمرارية أعمال المؤسسة.

يجب أن تصبح هذه الخطة المتفق عليها أو المقبولة لاستمرارية الأعمال BCP فيما بعد بمثابة حجر الأساس لجميع أنشطة التخطيط لاستمرارية المؤسسة. وهذا هو جوهر مفهوم الحوكمة الذي سوف يسمح للمؤسسة بتضمين خطط استمرارية الأعمال في ثقافتها العامة. كما يجب استخدامها من قبل المواد الإرشادية الخاصة باستمرارية الأعمال التي تمت مناقشتها في هذا الفصل في خطوة أولية لإطلاق مجموعة من العمليات الفعالة لإدارة استمرارية الأعمال (Business Continuity Management (BCM. وكما ذكرنا سابقاً، لا بد أن نرى هذا القالب، أو غمطاً قريباً جداً منه في أقرب وقت ممكن، وقد أصبح معياراً عالمياً لعملية استمرارية الأعمال، تماماً كإطار عمل الرقابة الداخلية الصادر عن لجنة

المنظمات الراعية (COSO) الذي تمت مناقشته في الفصل الرابع من هذا الكتاب والذي أصبح معياراً عالمياً.

يلخص نموذج دورة حياة إدارة استمرارية الأعمال BCM الموضح في الشكل التوضيحي (٣-١٠) العمليات الضرورية لفهم التنظيم النمطي للأعمال. ونتيجة لذلك يجب أن تكون المؤسسة في وضع يمكنها من اختيار إستراتيجيات ملائمة لاستمرارية أعمالها حتى تتمكن من تحقيق الأهداف المرجوة من وضع خطة لاستمرارية الأعمال BCP. كما يجب على المؤسسة إطلاق مجموعة من العمليات البديلة للتشغيل لكي يتم استخدامها بعد الانقطاع الناتج عن عطل ما وذلك للإبقاء على أنشطة الأعمال في كل مجال من المجالات الرئيسية. وبناء على المخاطر التي تم تقديرها، فإن هذه الإستراتيجيات يجب أن تعتمد على مجموعة من العوامل، في تحديد أطول فترة زمنية مسموح بها لتوقف بعض الأنشطة الحرجة، وتكلفة تطبيق الإستراتيجية بالإضافة إلى العواقب الناتجة عن أي عطل أو انقطاع.

إن الفرق الجوهرى بين اتباع هذا النموذج الخاص بخطة استمرارية الأعمال BCP والطرق التقليدية القديمة للتعافي من الكوارث، هو أن المخططين يجب أن لا يفكروا بخطة إستراتيجية واحدة للمؤسسة فحسب، بل لا بد من التفكير في كثير من الطرق المختلفة على مستوى النشاط بالنسبة للمؤسسة. إن التعقيدية الخاصة بالاعتمادات المتبادلة فيما يتعلق بالخدمات، وعمليات الأعمال، والبيانات، والتقنيات تحتاج إلى تحليل، وذلك من خلال الوسائل المناسبة لمعالجة احتياجات كل من:

• **الأشخاص في المؤسسة:** هناك حاجة لتحديد إستراتيجيات ملائمة للحفاظ على المهارات والمعرفة الأساسية للأفراد داخل المؤسسة ومستوى المعرفة لدى الأشخاص العاملين في المؤسسة والحفاظ عليها. فالعديد من هذه الاحتياجات هنا تشمل مجالات مثل أوصاف وظيفية موثقة، تدرج في التخطيط، والعديد من الممارسات الأخرى التي يجب تعزيزها من قبل الإدارة الجيدة للموارد البشرية. من ناحية أخرى يجب أن تدرك إستراتيجيات الأعمال دائماً أن الأفراد الأساسيين قد لا يكونون متاحين لمواصلة النشاط، وأن عمليات الاستمرارية القائمة على الأفراد يجب أن تكون دائماً في موضع التنفيذ.

- **احتياجات موقع العمل:** يجب على المؤسسة وضع إستراتيجية للتقليل من الآثار المترتبة على عدم إتاحة مواقع العمل الطبيعية. ويتطلب ذلك في معظم الحالات إستراتيجية لتحديد مواقع بديلة لاستمرار العمليات التشغيلية أو حتى تحديد أحد الموظفين للعمل من المنزل للقيام ببعض الأنشطة. فإذا كانت بعض مرافق المؤسسة قد تم تضمينها في أنشطة مثل الصناعات الثقيلة أو المعالجة الكيميائية، مهما يكن، فإن إتاحة موقع بديل ربما لا يكون بالأمر السهل، بل إن إستراتيجيات أخرى على مستوى النشاط قد تتضمن حتى الانسحاب من عمليات التشغيل على المدى القصير.
- **التقنيات الداعمة:** تعتمد المؤسسات على مرافق تقنية المعلومات ومعالجات شبكة الاتصالات السلكية واللاسلكية وموارد فحص المنتجات وعلى العديد من الأجهزة الأخرى حسب المنتج أو النشاط. وعلى الرغم من أن العديد من المؤسسات قد قامت بالفعل بتطوير خطط قوية للتعافي من كوارث تقنية المعلومات، فإن هذه المؤسسات بحاجة إلى فهم الأنشطة الأخرى لديها والقائمة على التقنية بشكل جيد لتقوم بتطوير إستراتيجيات مناسبة لخطط استمرارية الأعمال BCP.
- **المعلومات الفعلية والافتراضية:** بالإضافة إلى موارد تقنية المعلومات وغيرها من الأدوات القائمة على التقنية، يجب أن يكون لدى المؤسسة مجموعة كبيرة من الأنشطة المتعلقة بالمعلومات التي يمكن تقديمها على هيئة نسخ حقيقية وكذلك نسخ افتراضية أو إلكترونية. كما يجب أن يكون لأي معلومة مطلوبة لتنفيذ أنشطة حساسة الضوابط الملائمة والخاصة بالسرية والنزاهة والإتاحة والتداول.
- **المعدات والأجهزة:** يجب على المؤسسة تحديد وحيازة مخزون الأجهزة والمعدات الأساسية التي تدعم الأنشطة الحساسة. فقد تتضمن الإستراتيجيات القائمة على النشاط تخزين الأجهزة في مواقع بديلة، أو عمل الترتيبات اللازمة مع الأطراف الثالثة لتسليم الأجهزة، أو حيازة أجهزة معينة في مستودعات منفصلة، أو تحديد مصادر توريد بديلة. ولأن الأنشطة الحساسة تعتمد على تجهيزات متخصصة، يجب تحديد أو إجراء الاستعدادات التعاقدية مع الموردين الرئيسيين الحاليين.

• أصحاب المصالح والشركاء والمقاولون: يجب على المؤسسة وضع استراتيجيات ملائمة لإدارة العلاقات مع أصحاب المصالح وشركاء الأعمال أو الخدمات والمقاولين الرئيسيين، لذا يجب على إستراتيجية إدارة استمرارية الأعمال BCM أن تأخذ بعين الاعتبار تلك الأطراف المعنية الرئيسية والعمل على حماية مصالحهم.

إن تطوير خطة استمرارية الأعمال والإستراتيجية الداعمة قد يكون في الواقع جهداً كبيراً لتغطية جميع أنشطة المؤسسة. لذا يجب على الخطة الشاملة لاستمرارية الأعمال BCP أن تنظر في جميع التهديدات الخاصة بالاستمرارية فيما يتعلق بالروابط والعلاقات بين جميع الأنشطة الرئيسية للمؤسسة. ونظراً لكثرة التداخلات في جميع أنواع عمليات التشغيل الخاصة بالأعمال، فإن هناك عدداً قليلاً قائماً بذاته، وأنشطة مستقلة تماماً.

إن الممارسات الفعالة لأمن تقنية المعلومات عبارة عن مجموعة من المهام المعقدة والتي تتطلب دعماً فنياً قوياً لتقنية المعلومات في المؤسسة. الأمر نفسه بالنسبة للتخطيط لاستمرارية الأعمال الذي يتطلب دعماً كاملاً من تقنية المعلومات والإدارة العليا. فضلاً عن أن كليهما يعد من المكونات الهامة في العمليات الفعالة لحوكمة تقنية المعلومات.

ملاحظات:

1. Computers at Risk: Safe Computing in the Information Age (Washington, DC: National Academies Press, 1990), <http://www.nap.edu/openbook.php?isbn=0309043883>.

٢. مختبرات ضمان المواصفات (LU) هي منظمة غير ربحية تختص باختبار واعتماد سلامة المنتج. وقد قامت باختبار المنتجات من أجل السلامة العامة لأكثر من قرن. www.ul.com/global/eng/pages.

3. Mariane Swanson and Barbara Guttman, Generally Accepted System Security Principles (GASSP), NIST, Version 2.0, June 1996, <http://csrc.nist.gov/publications/PubsSPs.html>.

٤. معهد التعافي من الكوارث الدولية، مدينة فولز تشيرش، ولاية فرجينيا الأمريكية www.drii.org.

۲۵۵

الفصل الحادي عشر

معايير أمن البيانات الخاصة بصناعة بطاقات الدفع (PCI DSS) وقواعد أخرى لحوكمة تقنية المعلومات

يعد معيار أمن البيانات الخاص بصناعة بطاقات الدفع Payment Card Industry Data Security Standard PCI DSS أحد أفضل الممارسات الخاصة بأمن المعلومات وكذلك معيار الصناعة المطلوب من قبل العديد من المؤسسات التي تتعامل مع معلومات أصحاب البطاقات بالنسبة للبطاقات الرئيسية كالسحب / الخصم debit، والائتمان credit، وبطاقات الدفع الآلي ATM والبطاقات المستخدمة في نقاط البيع Point-Of-Sale (POS) الموجودة في محلات بيع التجزئة. وقد تم تعريف هذا المعيار من قبل مجلس معايير صناعة بطاقات الدفع وأمن البيانات PCI Data Security Standards Council، وقد تم وضع هذا المعيار لزيادة الضوابط التي تحيط ببيانات حامل البطاقة وتقليل عمليات الاحتيال على البطاقات الائتمانية، وذلك باستخدام مجموعة من أفضل الممارسات الموصى بها. ففي ظل الاعتماد على استخدام بطاقات الدفع في مختلف أشكال الأعمال التجارية في جميع أنحاء العالم هذه الأيام، ينبغي على المؤسسات التي تستقبل البطاقات الائتمانية لإتمام عملياتها التشغيلية على مختلف المستويات أن تلتزم بمعيار PCI DSS. إن فهم هذا المعيار ومتطلبات الامتثال به يعتبر واحد من العناصر الهامة الخاصة بحوكمة تقنية المعلومات بالنسبة للعديد من كبار مديري الأعمال هذه الأيام.

يقدم هذا الفصل معيار أمن البيانات الخاص بصناعة بطاقات الدفع PCI DSS، ويناقش أيضاً أهدافه الرقابية للمساعدة في بناء وصيانة شبكة آمنة لتقنية معلومات. وسنتحدث أيضاً عن متطلبات الامتثال التي تندرج تحت هذه القواعد، وكل من عمليات التقييمات المناسبة للأمن في المؤسسات الكبيرة إلى جانب عمليات الاستخدام الاختياري أو التطوعي لاستبيانات التقييم الذاتي (SAQ) Self-Assessment Questionnaire المتعلقة بمعيار PCI DSS في الشركات الصغيرة. وتشتمل قواعد هذا المعيار على ما هو أكثر بكثير

من مجرد المعاملات الخاصة بالبطاقات الائتمانية للعملاء، حيث يعد الامتثال هنا جزءاً رئيسياً وهاماً في حوكمة تقنية المعلومات.

كما يتحدث هذا الفصل أيضاً بشكل مختصر عن قانونين آخرين من القوانين الأمريكية التي لها تأثير في حوكمة تقنية المعلومات وهما: قانون غرام ليتش بليلي (Gramm-Leach-Bliley) الذي يغطي العمليات الخاصة بجمع المعلومات الشخصية الخاصة بالمستهلكين والإفصاح عنها وحمايتها، بالإضافة إلى مناقشة القواعد الخاصة بحفظ سجلات تقنية المعلومات التي تعد من عناصر قانون الرعاية الصحية المعروف بقانون HIPAA. إن نقاشنا الدائر حول كل من GLBA و HIPAA يعد مجرد أمثلة للعديد من القوانين والقواعد التي نواجهها اليوم والتي تشتمل على العديد من قضايا حوكمة تقنية المعلومات.

في الولايات المتحدة الأمريكية والاتحاد الأوروبي وغيرها من الأماكن في كل أرجاء العالم، نلاحظ أن تلك القوانين، وهذا العدد غير المحدود كما يبدو من القوانين والقواعد والمعايير الأخرى التي قد تم إصدارها مؤخراً؛ تحتوي على الأقل على بعض القضايا المتعلقة بحوكمة تقنية المعلومات. وفضلاً عن المعلومات الموجودة في ثنايا هذا الفصل حول PCI DSS و GLBA و HIPAA، فإن الفصول الأخرى ستقوم بتغطية القواعد والمعايير المختلفة لحوكمة تقنية المعلومات. على سبيل المثال، قدم الفصل السابع من هذا الكتاب المعايير الدولية الصادرة عن الآيزو فيما يخص حوكمة تقنية المعلومات، كما سيناقش الفصل السابع عشر من هذا الكتاب الإرشادات الخاصة باتفاقيات مستوى الخدمة لتقنية المعلومات وكذلك الإرشادات الخاصة بقيمة تقنية المعلومات Val IT الصادرة عن جمعية ISACA، وكلاهما هام جداً بالنسبة لحوكمة تقنية المعلومات. لذا ينبغي دائماً على القائمين على تقنية المعلومات المؤسسية أن يكونوا على الأقل على علم بتلك القوانين والقواعد وغيرها من المعايير الجديدة ومدى تأثيرها في الممارسات الجيدة لحوكمة تقنية المعلومات.

معلومات أساسية عن صناعة بطاقات الدفع وأمن البيانات PCI DSS والمعايير الخاصة بها:
بدايةً من مطلع ستينيات القرن الماضي، أصبحت بطاقات الائتمان البلاستيكية ذات النقوش البارزة من الأدوات الشائعة وقتها والتي استُخدمت بشكل أساسي من قبل رجال

الأعمال والمهنيين لشراء تذاكر الطيران، ودفع فاتورة عشاء العمل، وشراء وقود السيارة. ولا تزال بعض الشركات الأولى في هذا المجال والمُصدرة لهذه البطاقات العامة موجودة حتى الآن، كشركة أمريكان إكسبريس American Express، في حين أن أنواعاً أخرى لبطاقات الائتمان كانت تحمل أسماء مثل كارت بلانش Carte Blanche ودينرز كلوب Diners Club لم يعد لها وجود في الوقت الراهن. وقد تم إصدار بطاقات أخرى لإحدى شركات الوقود أو أحد المحلات التجارية، وكانت تلك البطاقات مفيدة فقط في شراء مثل هذه المنتجات أو في التعامل مع هؤلاء التجار. وقد كانت البطاقة الخاصة بشركة أمريكان إكسبريس رائجة بشكل بارز نظراً لاستخدامها لدى العديد من التجار الذين اتفقوا على قبول التعامل بها. إلا أن إصدارها ظل مقتصرًا على النخبة الذين تتوافر لديهم المعايير الائتمانية الشخصية القوية والمفروضة على إصدار مثل هذا النوع من البطاقات.

في سبعينيات القرن الماضي، ظهرت بطاقات الائتمان فيزا Visa وماستر كارد MasterCard، ومع مطلع الثمانينيات من القرن نفسه ظهرت بطاقة الائتمان ديسكفر Discover. حيث تم ترخيص وإصدار كل بطاقة من هذه البطاقات عن طريق البنك المحلي الخاص بحاملي هذه البطاقات بحيث تتبع لمجموعة مستقلة تكون مسؤولة عن إدارة العلامة التجارية الخاصة بالبطاقة ورسوم استخدامها في الأعمال التجارية التي تقبل تلك البطاقة. وقد شاع استخدام تلك البطاقات الائتمانية، بحيث أصبح العديد من المستهلكين هذه الأيام يحملون في جيوبهم عدداً كبيراً من البطاقات التي تصدر من بنوك مختلفة.

ازدهرت البطاقات الائتمانية ونجحت في جميع أنحاء العالم، وقد صاحب ذلك (الازدهار) زيادة مستوى المخاطر التي تتعلق بالاحتيايل على البطاقات الائتمانية وأمنها وحمايتها. وبالرغم من أن البنك هو المسؤول عن إصدار مثل تلك البطاقات الائتمانية للأشخاص، فإنه قد تم إنشاء شركات مستقلة لإدارة كل علامة من هذه العلامات التجارية الكبرى الخاصة بتلك البطاقات. فعلى سبيل المثال، تقوم إحدى هذه الشركات بالتعامل مع جميع بطاقات فيزا كارد Visa Card، في حين أن هناك شركة أخرى تتعامل مع بطاقات ماستر كارد MasterCard. أما فيما يخص أمن تلك البطاقات فقد كانت هناك اهتمامات تكاد تكون متشابهة بين تلك الشركات المعنية بإدارة كل بطاقة من هذه البطاقات، وذلك لإيجاد مستوى إضافي من الحماية بالنسبة للشركات المُصدرة لتلك البطاقات، وذلك عن طريق

ضمان أن التجار المتعاملين معهم لابد أن يلتزموا على الأقل بالحد الأدنى من مستويات الأمن عند قيامهم بحفظ ومعالجة ونقل البيانات الخاصة بحاملي تلك البطاقات.

ولإيجاد حل لتلك الاختلافات البسيطة الموجودة بين مختلف أنواع البطاقات الائتمانية على نحو أفضل، فقد تم تشكيل مجلس صناعة بطاقات الدفع Payment Card Industry (PCI) council. وقد كانت قضايا الأمن واختلاف القواعد أحد أبرز المشكلات المثارة بين جميع أعضاء المجلس. وفي عام ٢٠٠٤ قامت شركات البطاقات الائتمانية بتوحيد جميع السياسات الفردية لكل منهم، وتشكيل مجلس المعايير الأمنية Security Standards Council والذي نتج عنه إطلاق الإصدار الأول من معيار أمن البيانات PCI DSS. وكان عبارة عن معيار وليس قانوناً، إلا أنه كان من المتوقع أن يلتزم به جميع التجار الذين يستخدمون بطاقات الائتمان.

وبالنظر إلى كل التغيرات التي جرت على العمليات الخاصة بمعالجة البطاقات الائتمانية في السنوات الأخيرة، من خلال مميزات مثل المعالجة اللاسلكية، والمخاطر الخاصة بالسرقة علاوة على سرقة أرقام البطاقات المرخصة والمخزنة في سجلات أعمال المؤسسة، وغيرها من مخاطر الاحتيال المتزايدة، لذا فقد مر معيار PCI DSS بعدة مراحل من المراجعات والتنقيحات منذ الإصدار الأول له. وقد يتحقق الالتزام بقواعد المعيار PCI DSS من خلال التقييمات الذاتية الاختيارية أو التطوعية بالنسبة لصغار مستخدمي PCI. إلا أن الامتثال بها يكون إلزامياً بالنسبة للشركات الكبيرة التي تقوم بمعالجة تلك البطاقات الائتمانية. وسواء كانت بطاقات الدفع تستخدم هذه الأيام من خلال اختصاصي تقنية المعلومات أو من خلال أي من عمليات تشغيل المؤسسة، فإنه ينبغي أن يكون لدى مسؤولي الأعمال التنفيذيين فهم عام لمعيار PCI DSS ومدى تأثيره في العمليات التشغيلية للمؤسسة على الأقل.

يستعرض الشكل التوضيحي (١١-١) المتطلبات ذات المستوى الرفيع الخاصة بمعيار PCI DSS والأهداف الرقابية المرتبطة به. سنتحدث بتفصيل أكثر في الأقسام التالية عن الغاية الكامنة وراء متطلبات هذا المعيار، وسنوضح المتطلبات الضرورية للحفاظ على بيانات حامل البطاقة، ثم سنقوم بالحديث عن طبيعة وأهمية عمليات التقييم الذاتي الخاصة بهذا المعيار. وستتناول فصول أخرى مواضيع مهمة جداً لتحقيق الامتثال الفعال لهذا المعيار. على سبيل

المثال، قد ناقش الفصل العاشر من هذا الكتاب القضايا المتعلقة بأمن تقنية المعلومات التي تعد من الأمور الهامة بالنسبة للحوكمة الفعالة لتقنية المعلومات. هذه القضايا نفسها على الدرجة نفسها من الأهمية فيما يتعلق بتحقيق الامتثال لمعيار PCI DSS.

بالإضافة إلى معيار أمن البيانات DSS، فقد قام PCI بإصدار معيارين آخرين لهما علاقة بهذا المعيار وهما:

١- معيار أمن التعاملات الخاصة بالأرقام الشخصية السرية الخاصة ببطاقات الدفع PIN Transaction Security (PCI PTS). وهي مجموعة من المتطلبات الأمنية التي ركزت على إدارة الأجهزة المستخدمة لحماية أرقام التعريف الشخصية Personal Identification Number (PIN) لحاملي البطاقات الائتمانية والأنشطة الأخرى المتعلقة بمعالجة عملية الدفع، متضمناً متطلبات تصميم وصناعة ونقل الجهاز إلى المنشأة التي ستقوم بتطبيقه.

شكل توضيحي (١-١١)

متطلبات معيار أمن البيانات الخاص بصناعة بطاقات الدفع PCI DSS والأهداف الرقابية المرتبطة به

الأهداف الرقابية	متطلبات المعيار PCI DSS
بناء شبكة آمنة والحفاظ عليها.	١. قم بتنصيب وصيانة بنية الجدران النارية لحماية بيانات حامل البطاقة. ٢. لا تستخدم القيم الافتراضية التي يوفرها المورد لتخصيص كلمات المرور وغيرها من معاملات الأمن في النظام.
حماية بيانات حامل البطاقة.	٣. قم بحماية البيانات المخزنة لحامل البطاقة. ٤. قم بتشفير انتقال البيانات الخاصة بحامل البطاقة عبر الشبكات العامة والمفتوحة.
اتباع برنامج لإدارة نقاط الضعف.	٥. قم باستخدام برمجيات محدثة بشكل منتظم للتخلص من الفيروسات وفحص جميع الأنظمة التي تكون عادة عرضة للبرامج الضارة. ٦. قم بتطوير وصيانة تطبيقات نظم آمنة.

٧. قم بقصر الوصول لبيانات حامل البطاقة فقط على الأعمال التي بحاجة إلى معرفة هذه البيانات.	تطبيق إجراءات وتدابير قوية وصارمة لضبط الوصول.
٨. قم بتخصيص معرف فريد ID خاص لكل شخص يمكنه الوصول للبيانات باستخدام الحاسب.	
٩. قم بتقييد الوصول الفعلي لبيانات حامل البطاقة.	
١٠. قم بتعقب ورصد كل عمليات الوصول لموارد الشبكة وبيانات حاملي البطاقات.	مراقبة وفحص الشبكات بشكل منتظم.
١١. قم بفحص نظم وعمليات أمن البيانات بشكل منتظم.	
١٢. قم بالحفاظ على السياسة التي تقيّم من خلالها أمن المعلومات.	الحفاظ على سياسة أمن المعلومات.

٢. معيار أمن المعلومات الخاص بتطبيقات الدفع (Payment Application (PA DSS. هذا المعيار يخص مطوري البرمجيات والقائمين على تكامل تطبيقات الدفع والتي تقوم بتخزين أو معالجة أو نقل بيانات حاملي البطاقات كجزء من عملية الترخيص أو الاتفاقيات التي تتم عند القيام ببيع هذه النظم أو توزيعها أو ترخيصها للآخرين.

وعلى الرغم من العلاقة الوطيدة بين هذين المعيارين الجديدين والمعيار PCI DSS، فإننا سنركز في حديثنا في هذا الفصل على معيار أمن البيانات الخاصة بصناعة بطاقات الدفع PCI DSS. والذي يعد من المعايير الهامة لحوكمة تقنية المعلومات في العديد من المؤسسات.

حماية بيانات حاملي البطاقات وبرامج إدارة الثغرات الأمنية:

من السهل نوعاً ما أن يقوم التاجر الصغير بإجراء جميع الترتيبات المصرفية الضرورية لتنفيذ المعاملات التي تتم من خلال بطاقة الفيزا أو بطاقة الماستر كارد أو غيرهما، ثم يقوم بعد ذلك بوضع أجهزة قارئ أو ما يسمى بأجهزة الماسحات الضوئية من أجل قبول تلك البطاقات لإتمام عمليات الدفع الخاصة بالمشترى. حيث يتم نقل معلومات الشراء الخاصة بالبطاقة إلى معالج خاص ببطاقات الائتمان، ثم يحصل التاجر على ثمن المنتجات التي تم شراؤها. ويتم تحميل فاتورة الشراء على حساب بطاقة الائتمان الخاصة بالمشترى. في هذه العملية الشائعة بكثرة، توجد مخاطرة من أكبر المخاطر الأمنية التي

يتم تجاهلها غالباً، وهي أنه من الممكن أن تتم سرقة رقم البطاقة الائتمانية إلى جانب البيانات التعريفية الخاصة بالعميل واستخدامها في أغراض غير مشروعة. نذكر هنا على سبيل المثال إحدى الحوادث التي تم فيها التبليغ عن اختراق ما يزيد عن مائة مليون سجل من السجلات الخاصة بمعلومات العملاء في الولايات المتحدة على مدار عامين بدأت من عام ٢٠٠٥ وانتهت في عام ٢٠٠٧^(١). كما أن الاستخدام غير المشروع لتلك الأرقام الخاصة بالبطاقات الائتمانية التي تم اختراقها سيعرض كلاً من التجار وشركات البطاقات الائتمانية وأصحاب البطاقات إلى المخاطر. إن الهدف الرئيسي لمعيار PCI DSS هو توفير حماية كافية لبيانات أصحاب البطاقات المحفوظة في النظام. قد يعتقد المرء أن النظم الخاصة بمزودي خدمات البطاقات كبطاقة الفيزا أو الماستر كارد والبنوك المنتسبة لها ستكون آمنة (كما تشترط اللوائح المصرفية)، وأنه من المتوقع أيضاً أن يقوم الفرد بحماية بيانات البطاقة الائتمانية الخاصة به أو بها. على أية حال، جرت العادة أن يقوم أصحاب المحال التجارية بمعالجة العديد من أرقام البطاقات الائتمانية مع مرور الوقت. فالمطلب الرئيسي لمعيار PCI DSS هو ضرورة أن تقوم المؤسسة بتأمين وحماية البيانات الخاصة بالبطاقات الائتمانية.

المشكلة هنا هي أن أصحاب المحال التجارية هم من يقومون في أغلب الأحيان بعمليات تأمين الكثير من البيانات الخاصة بالبطاقات الائتمانية لعملائهم بصورة غير كافية. وفي جزء من الدراسة الكبرى التي جرت عام ٢٠٠٧ عن أصحاب المحال التجارية في الولايات المتحدة الأمريكية والاتحاد الأوروبي، وجدت الشركة الاستشارية فورستر^(٢) Forrester أن أصحاب المحال التجارية يقومون عادة بالاحتفاظ بكميات هائلة من البيانات الخاصة بالبطاقات الائتمانية الخاصة بعملائهم، وتشتمل هذه البيانات على أرقام البطاقات وتواريخ انتهائها وأسماء وعناوين أصحابها. تحتفظ المؤسسات عادة بمعلومات أكبر بكثير من مجرد أرقام البطاقات الائتمانية، ولا سيما تواريخ انتهاء البطاقات والأسماء والعناوين والرموز الأمنية. وفي ظل الافتقار إلى التدابير والإجراءات الأمنية القوية لتقنية المعلومات المؤسسية، قد يؤدي هذا التأمين الضعيف لمعلومات بطاقات الائتمان إلى العديد من الاختراقات والمشاكل الأمنية الجسيمة.

في أغلب الأحيان نجد أنه إما أن تكون عمليات التشفير والضوابط الأمنية الأخرى ضعيفة أو حتى غير مطبقة. وفي بعض الأحيان يمكن أن تواجه المؤسسات التي تقوم بمعالجة حجم هائل من المعاملات مخاطر ناجمة عن التراخي في عمليات معالجة المسائل الضرورية المتعلقة بالبطاقات الائتمانية للعملاء. وأمثلة على المخاطر والمشاكل يمكن مشاهدتها من خلال الأحداث التي وقعت في شركات تي جاي إكس TJX عام ٢٠٠٣، والتي تمتلك نحو ٢٥٠٠ متجر من متاجر التجزئة. فقد تم اختراق نظم الحاسبات الخاصة بها للمرة الأولى بواسطة أحد قراصنة (Hacker) شبكة الإنترنت الذي تمكن من اختراق النظام والوصول إلى معلومات تتعلق بالتعاملات الخاصة بالبطاقات الائتمانية للعملاء، وقد استمر ذلك لعدة شهور إلى أن تم اكتشاف أمره في عام ٢٠٠٦^(٣). وقد اشتملت تلك المعلومات على أسماء العملاء وأرقام بطاقات الائتمان الخاصة بنحو ٤٥,٧ مليون بطاقة سحب وائتمان تم سرقتها من خلال معاملات تمت خلال الفترة من شهر يناير إلى شهر نوفمبر من السنة نفسها. فقد ضاعت خصوصية بطاقات الائتمان لدى العديد من العملاء، وتعرضت شركة TJX لخسائر هائلة سواء كانت على الصعيد المادي جراء دعاوى التسوية القضائية أو على الصعيد الخاص بسمعتها.

إن تلك الواقعة الخاصة بشركات TJX ما هي إلا أحد الأمثلة على المخاطر التي يمكن أن تتعرض لها المؤسسة في حال كانت الضوابط الخاصة ببطاقة الائتمان لديها ضعيفة. ومن المؤكد أن يُظهر لنا تحليل الأحداث الخاصة بمثل هذه الاختراقات الأمنية مجموعة من نقاط الضعف الأمنية الشائعة التي يتم معالجتها الآن من خلال معيار PCI DSS. فقد تم تصميم نوع خاص من الضوابط الأمنية لتقنية المعلومات، وهو معيار PCI DSS والذي يشتمل على متطلبات تفصيلية، تحديداً، لهذا النوع من المخاطر - لتقليل فرص التعرض لإفشاء (تسريب) أو سرقة البيانات وكذلك تقليل التأثير الناتج جراء هذه السرقة أو إفشاء البيانات في حال وقوعه. تُظهر التحقيقات التي تتم بشكل مستمر بعد هذه التعرضات للمخاطر الخاصة بإفشاء البيانات أو سرقتها، بعض وليس كل الانتهاكات الشائعة الخاصة بمعيار PCI DSS وهي:

- ضوابط غير كافية على عملية الوصول للبيانات، وذلك من خلال التركيب غير السليم من قبل أصحاب المحال التجارية لنظم نقاط البيع POS، الأمر الذي يسمح للمستخدمين الأشرار من الوصول إلى المسارات التي تستهدف موردي نقاط البيع POS.

- الافتقار إلى التقنيات الخاصة بعمليات التسجيل أو المتابعة، مثل النظم الخاصة بمراجعات السجلات والكشف عن التسلات ومنعها، والنظم المساعدة في إجراء المسوحات الربع السنوية لنقاط الضعف، والنظم المسؤولة عن متابعة سلامة الملفات.
 - تخزين بيانات الشريحة الممغنطة لبطاقات الائتمان. فالعديد من الكيانات التي تم إفشاء بياناتها لا يعلمون أن الأنظمة التي لديهم تقوم بحفظ مثل تلك المعلومات، مما يوفر كمية هائلة من المعلومات للمتسللين.
 - عدم تغيير الإعدادات وكلمات المرور الافتراضية عند تركيب النظام. هذا بالإضافة إلى عدم إزالة الخدمات غير الضرورية وغير الآمنة أو تأمينها أثناء تثبيت النظام.
 - تطبيقات الويب سيئة التشفير تؤدي إلى نقاط ضعف قد تسمح بالوصول إلى قاعدة البيانات التي تحتفظ ببيانات أصحاب البطاقات من إحدى مواقع الإنترنت بشكل مباشر.
 - التطبيق السيئ للضوابط الخاصة بالتطبيقات الشبكية، الأمر الذي يعرض البيئة الخاصة ببيانات أصحاب البطاقات عن غير دراية إلى نقاط الضعف الموجودة في أجزاء أخرى من الشبكة التي لم يتم تأمينها بعد، كنقاط الاتصال اللاسلكية غير المؤمنة والثغرات الناجمة عن استخدام الإيميل وتصفح الإنترنت.
- لسنا هنا بصدد تقديم درس تعليمي حول القضايا الأمنية الخاصة بتقنية المعلومات، وإنما بصدد تأكيد أن أمن تقنية المعلومات هو أحد العناصر الهامة في حوكمة تقنية المعلومات، وأنه أيضاً أحد العناصر الحساسة في المعاملات المتعلقة بالبطاقات الائتمانية. إذ يستطيع المدير الأول (الأعلى) الاستعانة بالنقاط السابقة ليقوم بتوجيه أسئلة تتعلق بأمن وسلامة العمليات التشغيلية في المؤسسة فيما يخص البطاقات الائتمانية. على كل حال، بما أن معظم معلومات بطاقات الائتمان يتم نقلها مباشرة من نقاط البيع حيث المكان الذي يتم فيه إتمام عمليات البيع عن طريق بطاقات الائتمان، فالقاعدة الأساسية التي يجب التأكيد عليها بالنسبة لأصحاب المحال التجارية هي عدم نقل تلك البيانات الخاصة بالبطاقات الائتمانية للعملاء داخلياً على الإطلاق.

متطلبات معيار PCI DSS:

يجب على المؤسسة اتباع الخطوات اللازمة لتحقيق الامتثال لمعيار PCI DSS، وذلك من خلال تضافر الجهود بين كل من العاملين في تقنية المعلومات، والتدقيق الداخلي، والقانونيين، والعاملين بالائتمان والشئون المالية. وقد تم تلخيص هذه الخطوات في الشكل التوضيحي (١١-١) حيث سيكون لهذا المعيار المتطلبات التالية:

• **بناء شبكة آمنة والحفاظ عليها:** تحدث الفصل العاشر من هذا الكتاب عن أهمية أمن تقنية المعلومات في المؤسسة. إلا أن قواعد معيار PCI DSS تشترط أمرين محددين هنا: الأول، هو أنه يجب على المؤسسة أن تقوم ببناء وتركيب إعدادات الجدران النارية على نظم تقنية المعلومات لديها وصيانتها، وذلك لحماية بيانات حاملي البطاقات الائتمانية. ويعتد مفهوم الجدران النارية من المفاهيم الشائعة بين العاملين في مجال أمن تقنية المعلومات، غير أن هذا الأمر قد لا يكون شائعاً لدى المسئول التنفيذي للأعمال. يمكننا النظر إلى الجدران النارية لتقنية المعلومات على أنها تشبه أبواب الخروج ذات الاتجاه الواحد الموجودة في معظم المسارح. حيث يستطيع الشخص المرور من خلال تلك الأبواب إلى الخارج في حال اندلاع حريق، ولا يستطيع أحد موجود في الخارج من استخدام تلك الأبواب للدخول. وبالرغم من أن الضوابط الخاصة بالجدران النارية أصبحت اليوم شائعة الاستخدام في العديد من بيئات أمن تقنية المعلومات، فإنه يتعين على المؤسسة التأكد من أنه قد تم تركيب وإعداد تلك الجدران النارية على عناصر نظم تقنية المعلومات لديها والتي تشمل البيانات الخاصة بالبطاقات الائتمانية.

بالإضافة إلى ذلك، لا يجب على المؤسسة أن تستخدم الإعدادات الافتراضية المقدمة من قبل المورد والخاصة بكل من كلمات المرور Passwords وغيرها من المعاملات والمحددات الأمنية الأخرى التي يقوم المورد بتقديمها. وهي ببساطة تعتبر من الممارسات الأمنية الجيدة التي يتم تجاهلها غالباً. فقد تطلب البرمجيات التي يتم توفيرها من قبل المورد من العملاء الجدد إدخال "١٢٣٤" كلمة مرور أولية عند الإعداد الأولي للتطبيق، ومن ثم تغييرها بمجرد تركيب التطبيق. وهناك العديد من المستخدمين الذين لا يحملون أنفسهم عناء تغيير كلمة المرور، وهو الأمر الذي يجعل النظام دائماً عرضة للاختراقات من قبل المتطفلين الساعين للوصول إلى البيانات.

• **حماية البيانات الخاصة بحاملي البطاقات الائتمانية:** هناك العديد من الضوابط الأمنية لتقنية المعلومات التي تدرج تحت هذا المطلب متضمناً ذلك، عمل نسخ احتياطية من البيانات لاسترجاعها عند الحاجة، وتشفير البيانات أثناء تخزينها ونقلها، وحفظ كل ما يتعلق بوسائط تقنية المعلومات الخاصة بأصحاب البطاقات الائتمانية في مواقع حقيقية مؤمنة. وتعد هذه الإجراءات الخاصة بحماية بيانات حاملي البطاقات الائتمانية من المطالب الهامة لحوكمة تقنية المعلومات.

• **اتباع برنامج يقوم بإدارة الثغرات أو نقاط الضعف:** تحدث الفصل الثامن من هذا الكتاب عن إدارة المخاطر الخاصة بتقنية المعلومات. وكان يجب أن يكون هناك تركيز بشكل خاص على التقنيات الخاصة بإدارة المخاطر وتقدير نقاط الضعف والثغرات الأمنية بالنسبة للبيانات الخاصة بالبطاقات الائتمانية المخزنة أو التي يتم معالجتها من خلال موقع المؤسسة. كما ينبغي أيضاً أن يقوم قسم تقنية المعلومات في المؤسسة باستخدام برامج محدثة بشكل دوري ضد الفيروسات للتنبؤ بالبرامج الضارة.

• **تطبيق إجراءات وتدابير قوية وصارمة لضبط الوصول للبيانات:** تعد العمليات القوية لأمن تقنية المعلومات من الأمور الضرورية لتحقيق هذا المطلب. حيث تُستخدم بعض التقنيات الرقابية الرئيسية لتحقيق ما يلي:

o فرض القيود على عمليات الوصول الحقيقية لبيانات أصحاب البطاقات الائتمانية.

o اقتصار عمليات الوصول إلى بيانات أصحاب البطاقات فقط على الأعمال التي تحتاج إلى تلك البيانات فعلاً.

o تخصيص معرف فريد Unique ID لكل شخص يصل إلى البيانات عبر الحاسب الآلي.

هذه هي بعض الضوابط الرئيسية الخاصة بعملية الوصول إلى تقنية المعلومات. ويمكن لمسؤولي الأعمال التنفيذيين أن يطلبوا من الموظفين المسؤولين عن أمن تقنية المعلومات تقديم شرح تفصيلي عن التقنيات المستخدمة لضبط عمليات الوصول إلى تقنية المعلومات في المؤسسة. وعلى الرغم من أن هناك العديد من المصادر المطبوعة وكذلك المنشورة على شبكة الويب بشأن معلومات حول الضوابط الخاصة بالوصول وأمن تقنية المعلومات،

فإن مؤلف هذا الكتاب قد قام بوضع كتاب آخر^(٤) حول تلك الموضوعات الموجهة لمدققي تقنية المعلومات، غير أنها قد تزود مسئولي الأعمال التنفيذيين ببعض الملخصات الجيدة عن المعلومات الأساسية لأمن تقنية المعلومات.

• **مراقبة وفحص الشبكات بشكل منتظم:** يجب على المؤسسة تعقب ومراقبة جميع عمليات ومحاولات الوصول إلى موارد الشبكة وبيانات أصحاب البطاقات الائتمانية. فبالإضافة إلى الشرط أو المطلب الخاص بالرقابة والتتبع، فإن معيار PCI DSS يشترط أيضاً أن تقوم المؤسسة بفحص النظم والعمليات الأمنية الخاصة بها بصورة منتظمة. وتكون هذه المهمة غالباً من مسؤولية وحدة التدقيق الداخلي ومدققي تقنية المعلومات المتخصصين. وسنناقش بمزيد بالتفصيل في الفصل التاسع عشر من هذا الكتاب قضايا التدقيق الداخلي الخاصة بحوكمة تقنية المعلومات.

• **اتباع سياسة لأمن المعلومات:** تدعو هذه السياسة الأخيرة الخاصة بمعيار PCI DSS المؤسسات إلى اتباع السياسات التي تعالج قضايا أمن المعلومات. وهذا مشابه جداً للعمليات الأخرى لحوكمة تقنية المعلومات التي تم الحديث عنها في العديد من الفصول المختلفة لهذا الكتاب. وتعد هذه السياسات من الأمور الهامة بالنسبة للمؤسسة للتعرف على أفضل الممارسات التي من الضروري تطبيقها، غير أنه من الضروري أيضاً إيصال تلك السياسات لجميع أصحاب المصالح لتكون قواعد عامة يجب اتباعها.

تعد الشروط أو المتطلبات الخاصة بمعيار PCI DSS التي تم ذكرها أعلاه أكثر تحديداً من الإرشادات العامة التي سيتم تناولها في هذا القسم. إذ إن أكثر مديري الإدارة العليا سيبحثون عن المعايير رفيعة المستوى. في حين سيبحث أخصائي أمن الحاسبات في تقنية المعلومات عن متطلبات أكثر تفصيلاً. على سبيل المثال، يحتوي الشكل التوضيحي (١١-٢) على الإرشادات الخاصة بمعيار أمن البيانات DSS لواحد من هذه المتطلبات. فهذه المعايير تكون على مستوى مدقق تقنية المعلومات الماهر أو المتخصص في أمن تقنية المعلومات. النقطة الرئيسية هنا هي أنه يجب على المؤسسة إيجاد بعض الإجراءات الرقابية القوية للمحافظة على الامتثال لقواعد معيار PCI DSS.

بالنسبة للمؤسسات المتوسطة والكبيرة التي مع الوقت قد اكتسبت الخبرة في بناء وتشغيل نظم تقنية المعلومات الخاصة بها، فقد تبدو تلك المتطلبات الخاصة بقواعد معيار PCI DSS أكثر قليلاً من الممارسات الجيدة للرقابة الداخلية والشائع استخدامها والتي تعتبر بمثابة متطلبات رئيسية لتحقيق الإمتثال لقانون SOx كما وضحنا في الفصل الثاني من هذا الكتاب. في جميع الأحوال فإن الاختلاف الرئيسي هنا هو أن المؤسسة لن تخضع أبداً لعملية التدقيق الخارجي اللازمة للتصديق على مستوى امتثالها لمعيار PCI DSS. وإنما تدعو المعايير في هذه الحالة معظم المؤسسات التي تمارس القليل من نشاط البطاقات الائتمانية للقيام بمراجعة وتأسيس امتثالها لمعيار PCI DSS، وذلك من خلال عملية التدقيق والتقييم الذاتي.

شكل توضيحي (٢-١١)

المتطلبات الخاصة بتتبع ومراقبة الوصول إلى موارد الشبكة وبيانات أصحاب البطاقات

١. وضع عملية لربط جميع العمليات التي يقوم بها كل مستخدم للوصول إلى مكونات النظام، خاصة تلك العمليات التي تتم من خلال الامتيازات الإدارية.
٢. تطبيق الرقابة الآلية للمسارات على جميع مكونات النظام لإعادة بناء الأحداث التالية: - جميع العمليات الفردية التي يقوم بها المستخدم للوصول إلى بيانات أصحاب البطاقات. - جميع الإجراءات التي ينفذها المستخدمون أصحاب الامتيازات الإدارية أو الأصلية. - الوصول إلى جميع مسارات التدقيق. - محاولات الوصول للمنطقية غير السليمة. - استخدام تقنيات التعريف والتوثيق. - تهيئة سجلات التدقيق. - إنشاء وحذف كائنات على مستوى النظام.
٣. القيام بتسجيل المدخلات ومسارات التدقيق المتعلقة بكل حدث من الأحداث التي تمت على جميع مكونات النظام، والتي تشتمل على الأقل على هوية المستخدم ونوع الحدث والوقت والتاريخ ومؤشر نجاح أو فشل الحدث وبداية الحدث وهوية كل من البيانات أو مكون النظام أو المورد الذي تأثر بهذا الحدث.

٤. باستخدام تقنية المزامنة، قم بمزامنة جميع الساعات والأوقات الحاسمة في النظام وقم بتطبيق ضوابط للحصول على الوقت وتوزيعه وحفظه.
٥. تأمين مسارات التدقيق بحيث لا يُسمح بتعديلها.
٦. مراجعة السجلات الخاصة بجميع مكونات النظام المتعلقة بالمهام الأمنية مرة في اليوم على الأقل.
٧. الاحتفاظ بتاريخ مسارات التدقيق لمدة عام واحد على الأقل، ولا بد أن يكون هناك سجلات لثلاثة أشهر على الأقل من التاريخ الحالي متاحة أو متوفرة للتحليل.

عملية التقييم الذاتي لمعيار PCI DSS:

لكي تتأكد المؤسسة من امتثالها أو اتباعها لبعض المتطلبات الخاصة بأحد المعايير، فمن الطبيعي ومن الضروري أيضاً الاستعانة بطرف خارجي لفحص هذا الامتثال والتأكد من مدى تطبيقه. على سبيل المثال، من الضروري أن يقوم المدققون الخارجيون (مكاتب التدقيق الخارجي) - مكاتب المحاسبة القانونية في الولايات المتحدة الأمريكية؛ بمراجعة القوائم المالية الخاصة بالمؤسسة والتصديق على مدى صحتها. ومن الضروري أيضاً أن يكون هناك مراجعون متخصصون مستقلون يقومون بمساعدة المؤسسة على التأكد من مدى امتثالها لأي معيار من معايير الأيزو متضمنة تلك التي تحدثنا عنها في الفصل السابع من هذا الكتاب. ولكن نظراً لوجود عدد كبير من المحال التجارية - الصغيرة نسبياً غالباً - التي تتعامل مع بيانات البطاقات الائتمانية، ونظراً لأن تكلفة الاستعانة بمراجعين خارجيين ستكون مرتفعة بعض الشيء؛ فقد سمحت منظمة المعايير الخاصة بصناعة بطاقات الدفع للمؤسسات بالقيام بتنفيذ نشاط التقييم الذاتي للتحقق من امتثالها للمعايير الصناعية.

إن استبيان أو استطلاع التقييم الذاتي (Self-Assessment Questionnaire (SAQ الخاص بمعيار PCI DSS ما هو إلا أحد الأدوات المستخدمة لمساعدة أصحاب المحال التجارية ومقدمي الخدمات على القيام بعملية تقييم ذاتي لمعرفة مدى التزامهم وامتثالهم لمعيار PCI DSS. ويمكننا إيجاد العديد من النسخ التفصيلية الخاصة بمعايير التقييم الذاتي من خلال زيارة الموقع www.pcisecuritystandards.org/security_standards/index.php. حيث تدعو تلك المعايير الخاصة بالتقييم الذاتي إلى ما يلي:

• بناءً على التوجيه الخاص بمجلس المعايير الأمنية الخاصة بصناعة بطاقات الدفع PCI حول "اختيار استبانة التقييم الذاتي والتصديق على أفضل تطبيق لها على المنظمة الخاصة بك". فإنه يجب على المؤسسة اختيار استبانة التقييم الذاتي المناسبة لمقدمي الخدمات وأصحاب المحال التجارية لديها.

• بعد اكتمال الاستبانة المناسبة للتقييم الذاتي SAQ بنجاح، تستطيع المؤسسة التصديق على شهادة ذاتية تدل على أنها مؤهلة لتنفيذ (بل وأنها نفذت) بالفعل نشاط التقييم الذاتي الخاص بالامتثال لمعيار PCI DSS.

طبقاً لمتطلبات المعايير الصناعية فإنه ينبغي على جميع المستخدمين الرئيسيين للبطاقات الائتمانية الاستعانة بمُقيّم مستقل للقيام بمراجعة هذا الامتثال، وهذا مشابه للمراجعات الخاصة بالامتثال بمعايير المنظمة الدولية للمواصفات والمعايير ISO التي تحدثنا عنها في الفصل السابع من هذا الكتاب. حتى بالنسبة للمؤسسات الأصغر حجماً، فإن الامتثال بمعايير أمن المعلومات ممكن أن يعود بالنفع والفائدة على أعمالها، في حين أن عدم الامتثال بها قد يؤدي إلى عواقب وخيمة وخطيرة طويلة الأجل. إن الامتثال بقواعد معيار PCI DSS هام للأسباب التالية:

• الامتثال لمعيار PCI DSS يعني أن النظم آمنة، وأنه يمكن للمستخدمين الوثوق بالمؤسسة فيما يتعلق بالمعلومات الحساسة الموجودة في بطاقتهم الائتمانية.

• الامتثال يحسن من سمعة ومكانة المؤسسة لدى المشتري وشركات المدفوعات من أصحاب العلامات التجارية - الشركاء الذين تحتاج إليهم للقيام بالأعمال التجارية.

الامتثال هو عملية مستمرة ودائمة، ولا يمكن أن تكون عبارة عن عملية تحدث مرة واحدة فقط. ويساعد الامتثال في منع المخالفات أو الاختراقات الأمنية الحالية والمستقبلية، كما يمنع سرقة بيانات بطاقات الدفع. ونظراً لأن عمليات إفشاء (تسريب) البيانات أصبحت الآن متطورة أكثر من أي وقت مضى، نرى أن مجلس المعايير الأمنية الخاصة بصناعة بطاقات الدفع PCI يعمل دائماً على مراقبة التهديدات وتحسين الوسائل الصناعية المستخدمة للتعامل معها، وذلك من خلال إجراء التحسينات على المعايير الأمنية الخاصة بصناعة بطاقات الدفع وإجراء التدريبات اللازمة للمختصين في المجال الأمني.

كم أن للامتثال فوائد غير مباشرة، فقد يساعد المؤسسة على أن تكون في وضع أفضل فيما يخص امتثالها بلوائح تنظيمية أخرى مثل قانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة (HIPAA) Health Insurance Portability and Accountability Act الذي سنتحدث عنه لاحقاً في هذا الفصل، وأيضاً كالامتثال لقانون ساربينز أوكسلي SOx الذي تطرقنا إليه في الفصل الثاني من هذا الكتاب. بعبارة أخرى، يمكن أن نقول إن هذا التقييم الذاتي قد يوفر القاعدة الأساسية للإستراتيجية الأمنية للشركة، وقد يحدد أساليب لتحسين فاعلية البنية التحتية لتقنية المعلومات.

قانون جرام ليتش بيلي (GRAMM-LEACH-BLILEY) في القواعد الخاصة بحوكمة تقنية المعلومات:

في أواخر تسعينيات القرن الماضي أقر مجلس النواب الأمريكي قانوناً لتغيير بعض القواعد المعمول بها في المؤسسات المالية القائمة منذ الكساد العظيم الذي حدث في ثلاثينيات القرن الماضي. وقد عُرف هذا القانون الجديد رسمياً باسم قانون تحديث القطاع المالي لسنة ١٩٩٩، والذي اشتهر أكثر باسم قانون جرام ليتش بيلي (Gramm Leach Bliley Act) GLBA. هذا القانون عبارة عن مجموعة من المتطلبات المتعلقة بالخصوصية والهادفة لحماية المعلومات المالية الشخصية الخاصة بعملاء المؤسسات المالية. ويتكون هذا القانون التشريعي المتعلق بالخصوصية من ثلاثة أجزاء رئيسية هي: (١) قاعدة الخصوصية المالية و(٢) قاعدة الحماية و(٣) ما يعرف باسم "أحكام التحجج الاحتيالي" (استخدام الأكاذيب للوصول لبيانات الآخرين) Pretexting provisions. بينما لم يسمع المهنيون قط بمفهوم "التحجج الاحتيالي" الذي جاء به هذا القانون، فإنه سيتم مناقشة هذا المفهوم واعتباراته الخاصة بحوكمة تقنية المعلومات الموجودة في مواد أخرى من هذا القانون في الأجزاء اللاحقة. يمنح هذا القانون GLBA السلطة إلى ثماني وكالات وولايات اتحادية أمريكية رسمية مختلفة للقيام بإدارته، كما يفرض هذا القانون أيضاً مجموعة جديدة من القواعد المتعلقة بالخصوصية التي يتم تطبيقها على المؤسسات المعروفة عموماً باسم "المؤسسات المالية". ولا نعني بهذه المؤسسات البنوك، وشركات التورق، وشركات التأمين التقليدية فحسب، ولكن نعني أيضاً المؤسسات التي تقدم لعملائها أنواعاً مختلفة من المنتجات

والخدمات المالية كخدمات الإقراض، والوساطة، ومختلف أنواع القروض الاستهلاكية، وخدمات نقل وحماية الأموال، وخدمات إعداد الإقرارات الضريبية الفردية، وخدمات تقديم النصائح المالية والاستشارات الائتمانية، وخدمات التأسيس العقاري السكني، وخدمات تحصيل القروض الاستهلاكية وغيرها من الخدمات المالية الأخرى. وفي ظل قانون GLBA فإن لجنة التجارة الاتحادية أو الفيدرالية (Federal Trade Commission) (FTC) هي التي تقوم الآن بالإشراف على تلك "المؤسسات المالية" غير التقليدية، سواء كان ذلك بشكل مباشر أو من خلال الوكالات الرسمية والاتحادية.

وعلى الرغم من أن المدير الأول الذي يعمل لصالح أحد البنوك أو شركات التأمين في الوقت الراهن قد يكون هو المعني بهذا القانون وبأحكام الخصوصية التابعة له، إلا أنه يمكن اعتباره القاعدة التي تستطيع التأثير في العديد من المؤسسات الأخرى، وذلك بسبب المعنى الواسع للمصطلح المعروف "بالمؤسسات المالية". وقد تم تطبيق قواعد هذا القانون على العديد من المؤسسات المالية الخاضعة للوائح الرسمية. على سبيل المثال، قد تم تنظيم شركات التأمين في الولايات المتحدة على أساس كل ولاية على حدة، وذلك من خلال الجمعية الوطنية لمفوضي التأمين (National Association of Insurance Commissioners (NAIC)، والتي تعمل بصفة مجموعة مركزية لتنسيق ووضع المعايير لتلك اللجان المعتمدة في الولاية. وأن هذا التحالف أو المجموعة NAIC هي التي تفرض قواعد التفويض الاتحادية لقانون GLBA على شركات التأمين المستقلة التابعة لها والمنظمة من قبل الولاية الموجودة فيها. وهذا مثال آخر يوضح كيف تنتقل اللوائح القانونية الاتحادية في الولايات المتحدة في بعض الأحيان من سلطة الدولة الأمريكية كهيئة الأوراق المالية والبورصة الأمريكية SEC، المعنية بأمور قانون SOX، إلى قواعد على مستوى قوانين الولاية الواحدة، هذا إلى جانب بعض القواعد المالية العالمية المشابهة. فنحن ننسى غالباً أن بعض اللوائح القانونية للشركات والعديد من المبادئ التشريعية الأخرى في الولايات المتحدة تكون فعالة طبقاً لكل ولاية على حدة. فعلى سبيل المثال، يتم إصدار رخص قائدي المركبات من قبل كل ولاية على حدة. وبالمثل، فإنه وعلى الرغم من أن إدارة الاختبارات الخاصة بالحصول على شهادة محاسب قانوني CPA تتم محلياً من قبل الجمعية الأمريكية للمحاسبين القانونيين AICPA، إلا أن رخص المحاسبين القانونيين CPAs يتم منحها تبعاً لكل ولاية عن طريق مجلس المحاسبة الخاص بالولاية. فمن خلال

سلطة الجمعية الوطنية لمفوضي التأمين، وهو الكيان المعني بتنسيق القواعد داخل الولاية، فقد تم تبني واعتماد قواعد قانون GLBA من قبل معظم الولايات في الولايات المتحدة الأمريكية.

قواعد الخصوصية المالية لقانون GLBA:

يواجه المستخدمون غالباً هذه الأيام داخل الولايات المتحدة قانون GLBA وقواعد الخصوصية المالية الخاصة به عند استلامهم إشعارات مفيدة من مقدم خدمة البطاقات الائتمانية تصف لهم قواعد الخصوصية الخاصة ببطاقتهم الائتمانية. حيث تشترط قواعد الخصوصية المالية لقانون GLBA من المؤسسات المالية أن تقوم بتزويد عملائها بإشعارات وملاحظات حول الخصوصية المالية المتبعة لديهم والتي توضح لهم الممارسات المتبعة في المؤسسة المالية لجمع وتبادل البيانات. ويجب أن يكون إشعار الخصوصية هذا واضحاً جداً وبارزاً وبه إفصاح دقيق عن ممارسات الخصوصية المتبعة في الشركة. كما يجب أن يحتوي هذا الإشعار على معلومات قامت الشركة بجمعها عن عملائها وكذلك من المستهلكين، وأيضاً معلومات تتعلق بالجهات التي تتبادل معها الشركة المعلومات الخاصة بالبطاقات الائتمانية، ومعلومات عن الكيفية التي تقوم بها الشركة بحماية وصيانة هذه المعلومات. يطبق الإشعار على "المعلومات الخاصة الشخصية" للمستهلكين والعملاء التابعين للشركة والتي تقوم الشركة بجمعها والإفصاح عنها، إلا أنه على الصعيد العملي يمكن أن يطبق على معظم أو كل بيانات العملاء الموجودة لدى الشركة. على سبيل المثال، المعلومات الشخصية الخاصة قد تكون المعلومات التي يقوم المستهلك أو العميل بإدخالها أثناء استخدامه لتطبيقات العقود الائتمانية أو عقود البيع، أو معلومات تتعلق بشخص ما يمكن الحصول عليها من مصدر آخر كالمكاتب الائتمانية، أو معلومات عن العمليات التي تتم بين الشخص والشركة كالمعلومة التي تتعلق بالرصيد الموجود في الحساب مثلاً. في الحقيقة واعتماداً على قانون GLBA يتم تصنيف المعلومات الخاصة بأي شخص يُدرج اسمه في قائمة العملاء أو المستهلكين التابعين لمؤسسة مالية محددة على أنها معلومات خاصة شخصية. ولا تخضع المعلومات التي تعتقد المؤسسة لسبب ما بأنها معلومات عامة قانونياً لقانون GLBA، مثل معلومات قروض الرهن العقاري في الجهة القضائية التي يتم تسجيلها علناً.

- وبناء على قانون GLBA فإنه يجب أن تحتوي إشعارات الخصوصية على المعلومات التالية:
- أنواع المعلومات الخاصة الشخصية للعملاء التي تقوم المؤسسة بجمعها.
- أنواع المعلومات الخاصة الشخصية للعملاء التي ستقوم المؤسسة بالإفصاح عنها للآخرين.
- الأطراف التي ستبيح لها المؤسسة الاطلاع على هذه المعلومات، من غير الأطراف الخاضعة للحظر في عدم الإفصاح عن المعلومات.
- أحقية العميل أو المستخدم بالاعتراض على الإشعار ووجود قواعد توضيحية بسيطة عن آلية رفع تلك الاعتراضات.
- السياسات المتبعة في المؤسسة بخصوص مشاركة بيانات شخص لم يعد الآن من أحد عملائها أو زبائنها.
- الإجراءات المتبعة في المؤسسة لحماية خصوصية وأمن المعلومات الخاصة الشخصية لزبائنها وعملائها.

لا يكثر الكثير من المستهلكين هذه الأيام بتلك الإشعارات، على الرغم من أنها يمكن أن تصرح عن رغبة الشركة المالكة للبيانات الخاصة بحسابات العملاء بالقيام بمشاركة اسم العميل مع الآخرين. فبدلاً من هذه الممارسة المستخدمة كثيراً من المستهلكين، والتي هي إتلاف وإهمال الإشعارات أو الملاحظات، فإن قانون GLBA يعطي الحق للمستهلك بأن يقوم بالاعتراض على قيام الشركة بمشاركة تلك المعلومات الخاصة به مع الأطراف الأخرى. ويجب أن يوضح الإشعار - وغالباً بطريقة معقولة ومنطقية - الطريقة التي يمكن اتباعها من قبل المستهلكين لتقديم اعتراضاتهم. على سبيل المثال، طريقة توفير رقم هاتف مجاني للاعتراضات والشكاوى أو توفير نموذج منفصل يحتوي على العنوان تعتبر من الطرق المعقولة للاعتراض بالنسبة للمستهلكين والعملاء، أما مطالبة الأشخاص بأن يقوموا بكتابة رسالة اعتراضية كوسيلة وحيدة لتقديم اعتراضاتهم لا تعتبر أبداً طريقة معقولة ومقبولة. كما يجب أن يوضح إشعار الخصوصية أيضاً أن للمستهلكين الحق (أن يقولوا لا) بالنسبة للسماح بمشاركة معلومات محددة تخصهم. مثل مشاركة معلومات تقرير أو تطبيق ائتماني مع الأقسام أو الفروع المستقلة عن المؤسسة المالية.

يضع قانون GLBA بعض القيود على الكيفية التي يمكن من خلالها لأي شخص يستقبل معلومات شخصية خاصة من إحدى المؤسسات المالية أن يقوم باستخدام تلك المعلومات أو إعادة الإفصاح عنها. فإذا قام المُقرض بالإفصاح عن معلومات العميل لمزود الخدمة المسؤول عن بيانات الحسابات البريدية - حيث لا يحق للعميل الاعتراض على ذلك - فإنه ينبغي على مزود الخدمة هذا أن يقوم باستخدام تلك البيانات لأهداف محددة فقط - كإرسال بيانات الحسابات البريدية - ولا ينبغي عليه بيع أو استخدام هذه البيانات لأغراض تسويقية.

إن مبدأ الخصوصية المالية الخاص بقانون GLBA سيكون أكثر تعقيداً عندما نخوض أكثر في أمور تفصيلية تابعة له. في جميع الأحوال، نحن لا نهدف هنا إلى عرض هذا الشرح التفصيلي المتعلق بتلك الجزئية من قانون GLBA، وإنما هدفنا هو فقط توضيح هذه القواعد المتعلقة بالخصوصية وتأثيراتها في حوكمة تقنية المعلومات بشكل عام. لذا يجب على مديري المؤسسات إدراك أن كل المعلومات الشخصية الخاصة تعد معلومات سرية للغاية ولا يمكن القيام ببيعها أو نشرها دون مبرر. وأن للمستهلكين أن يعترضوا وأن يقولوا لا، ويجب على المؤسسة الاحتفاظ بشكل ملائم بتلك السجلات الخاصة بالاعتراضات المقدمة، وأن يتم احترام حقوق المستهلكين في الخصوصية. وينطبق الأمر نفسه على أي مؤسسة تقدم تسهيلات منح ائتمانية ودفع فواتير خاصة بالمستهلكين. وتُعَرِّض المؤسسة نفسها للمخاطر عندما تتعامل مع مبدأ الخصوصية الخاص بقانون GLBA كما لو كان عبارة عن أمر بسيط أو تافه أو إلى حد ما هام، فعدم الالتزام والإخلاص في التعامل مع أي من طلبات الاعتراضات المقدمة، أو البيع غير الصحيح للقائمة البريدية، قد يعرض المؤسسة إلى رفع بعض أنواع الدعاوى القضائية جراء الأضرار الناجمة عن عدم الالتزام بمبدأ الخصوصية الخاص بهذا القانون.

قاعدة الحماية في قانون GLBA:

إن قاعدة الأساليب الوقائية لقانون GLBA تطلب من المؤسسات المالية بأن يكون لديها خطة أمنية معمول بها لحماية خصوصية وسلامة المعلومات الشخصية للعملاء. فعندما يقوم العملاء بفتح حسابات جديدة، أو يقوموا بإجراء عمليات شراء منتجات، فإنهم يفصحون عن بعض معلوماتهم الشخصية، كالعنوان ورقم الهاتف أو رقم بطاقة

الائتمان كجزء من إجراء المعاملات الخاصة بالتطبيق. لذا يجب أن يكون لدى المؤسسة خطة أمنية معمول بها لحماية سرية وسلامة هذه البيانات الشخصية التي قام المستهلك بالإفصاح عنها. كما يجب أن تشتمل هذه الخطة على ما هو أكثر من مجرد مخاطر متعلقة باستمرارية الأعمال، التي تحدثنا عنها بإيجاز في الفصل العاشر من هذا الكتاب، بل يجب أن تشتمل أيضاً على ضوابط خاصة لمنع القراصنة hackers من الوصول إلى ملفات البيانات، ومنع الموظفين الموترين أو الناقمين من الوصول إلى معلومات العملاء، ومنع أي تهاون حتى لو كان بسيطاً. كما تطلب قاعدة الأساليب الوقائية الخاصة بقانون GLBA من كل مؤسسة مالية، بغض النظر عن حجمها، بل وتفرض عليها بأن تقوم بوضع وتنفيذ خطة مكتوبة لأمن المعلومات لحماية بيانات العملاء. بحيث يتناسب نطاق هذه الخطة الأمنية ودرجة تعقيدها تناسباً طردياً مع حجم المؤسسة وحساسية المعلومات التي تحتفظ بها. ويجب أن تكون هذه الخطة قائمة على عملية تحليل المخاطر التي تعمل على تحديد كل التهديدات المتوقعة بالنسبة لأمن وسرية وخصوصية وسلامة معلومات العملاء. وبناء على هذه العملية التحليلية للمخاطر، فإنه ينبغي على المؤسسات المالية توثيق وتطبيق التدابير والإجراءات الأمنية، التي تتضمن أيضاً التدابير والإجراءات الإدارية مثل تدريب الموظفين على وسائل الحماية التقنية، متضمناً ذلك تدريبات حول استخدام كلمات المرور وضوابط التشفير والجدران النارية. كما تشتمل هذه التدابير والإجراءات الأمنية كذلك على الاحتياطات الوقائية المادية مثل الأقفال الموجودة على الأبواب وأجهزة الحاسب الآلي. كما يجب على المؤسسات المالية أن تقوم بتخصيص واحد أو أكثر من موظفيها لكي يقوم بتنسيق وتنظيم تلك الأساليب الوقائية. كما يتعين على تلك المؤسسات أيضاً القيام بإجراء مراجعات دورية لتحديد ما إذا كانت البرامج الأمنية المتبعة فيها جيدة أم بحاجة إلى تعديل في ظل الظروف المستجدة.

تستطيع المؤسسة أن تثبت امتثالها للقاعدة الخاصة بالأساليب الوقائية من قانون GLBA من خلال الخطوات التالية:

١- تحليل المخاطر البيئية المحيطة: يجب على المؤسسة أن تحدد بشكل رسمي جميع المخاطر الداخلية والخارجية المتعلقة بأمن وخصوصية وسلامة المعلومات الشخصية

لجميع العملاء. وقد سبق الحديث عن الطرق التحليلية للمخاطر في الفصل الثامن من هذا الكتاب. ويجب أن تغطي تلك العملية التحليلية مخاطر أو فقدان أو الإفصاح عن جميع مصادر المعلومات الشخصية، سواء كانت موجودة على الأنظمة الآلية أم في السجلات اليدوية.

٢- **تصميم وتطبيق الإجراءات الوقائية:** إن الإجراءات الوقائية هي بالأصل عبارة عن إجراءات الرقابة الداخلية التي تم الحديث عنها في الفصل الرابع من هذا الكتاب كجزء من إطار الرقابة الداخلية الخاص بلجنة المنظمات الراعية (COSO).

٣. **المتابعة والتدقيق:** يجب أن تكون هناك عمليات متابعة مستمرة لضمان القيام بعمليات التدقيق. كما يتعين على الإدارة العليا تشجيع مدققيهم الداخليين بأن يضعوا جدولاً زمنياً منتظماً لسلسلة من المراجعات للتحقق من مدى ملاءمة أو كفاية خطة أمن المعلومات في المؤسسة إلى جانب اختبارات الامتثال المناسبة.

٤. **برنامج ثابت للتحسينات:** نتيجة منطقية لأي نقطة ضعف أو ثغرة يتم الإبلاغ عنها من خلال عمليات التدقيق أو أي فحوصات أخرى، فإنه يجب أن يكون لدى المؤسسة برنامج معمول به يعمل بشكل مستمر على إجراء التحسينات اللازمة على خطة أمن المعلومات لديها. ويجب أن يكون هذا البرنامج موثقاً جيداً وأن يصف التحسينات التي طرأت على الخطة.

٥. **الإشراف على مزودي خدمات أمن المعلومات والشركاء:** قد يكون للعديد من الشركاء والمؤسسات الأخرى أحقية الوصول إلى المعلومات الشخصية تلك نفسها، أو ربما يكون لديهم فقط إمكانية الدخول إلى وصلات شبكات النظم التي يمكن من خلالها انتهاك الخصوصية الشخصية للبيانات. فهناك حاجة لسياسات وضوابط وإجراءات تدقيق ملاءمة معمول بها على نحو جيد لمنع الانتهاكات.

تُطبق قاعدة الأساليب الوقائية لقانون GLBA على مجموعة كبيرة من مزودي المنتجات والخدمات المالية، متضمنين وسطاء الرهن العقاري وجهات الإقراض غير المصرفية والمؤمنين ووكالات إعداد التقارير الائتمانية ومعدّي الضرائب المهنية، هذا بالإضافة إلى تجار التجزئة الذين يقومون بإصدار بطاقات ائتمانية خاصة بهم وبأعمالهم. ولا تخضع البنوك لقاعدة

الأساليب الوقائية الخاصة بقانون GLBA، ولكنها يجب أن تمتثل للوائح تنظيمية مناظرة أو مشابهة لها قد تم إصدارها من قبل الوكالات الاتحادية للأعمال المصرفية. وقد ينتج عن عدم الامتثال لقاعدة الأساليب الوقائية لقانون GLBA فرض الغرامات أو بعض الإجراءات التنفيذية من قبل هيئة التجارة الفيدرالية (Federal Trade Commission (FTC.

قوانين حظر التحجج الاحتياطي pretexting في قانون GLBA:

يمنع قانون GLBA "التحجج الاحتياطي" - ذلك التعبير الذي يشير إليه المدقق الإملائي في برنامج معالج النصوص وورد Word على أنه خطأ إملائي - والذي يقصد به استخدام الادعاءات والأساليب الكاذبة، متضمناً ذلك استخدام البيانات المزورة، أو القيام بانتحال شخصية ما من أجل الحصول على المعلومات المالية الشخصية الخاصة بالعملاء، مثل معرفة الأرصدة البنكية الخاصة بهم. حيث يقوم المزورون أو المخادعون باستخدام مجموعة متنوعة من الأساليب للحصول على المعلومات الشخصية. على سبيل المثال، قد تقوم إحدى المخادعات بإجراء مكالمة هاتفية تدعي فيها العمل لدى شركة تقوم بإجراء دراسات استقصائية، ثم تقوم بطرح بعض الأسئلة التي تهدف من خلالها إلى الحصول على اسم أحد البنوك على سبيل المثال، ثم تقوم بعد ذلك باستخدام تلك المعلومات التي قامت بالحصول عليها لتقوم بإجراء مكالمة هاتفية مع المؤسسة المالية التي تحتفظ بمعلومات الشخص المستهدف متظاهرة بأنها هي ذلك الشخص المستهدف أو بأنها هي الشخص الذي يملك صلاحية الوصول إلى حسابه. وقد تدعي بأنها نسيت دفتر الشيكات الخاص بها وأنها بحاجة لمعلومات عن الحساب. فبهذه الطريقة قد تتمكن تلك المخادعة من الحصول على بعض المعلومات الشخصية للضحية المستهدفة كرقم الضمان الاجتماعي أو رقم الحساب البنكي أو رقم بطاقة الائتمان أو معلومات عن التقارير الائتمانية أو وجود وحجم المدخرات الشخصية والمحافظ الاستثمارية.

وبموجب أحكام قانون GLBA الخاصة بالادعاءات الاحتياطية، فإنه من غير القانوني لأي شخص:

- أن يستخدم بيانات أو وثائق مزورة أو وهمية أو مخادعة للحصول على أي معلومات شخصية للعملاء من المؤسسة المالية أو من عميل المؤسسة المالية بشكل مباشر.

- أن يستخدم وثائق مزيفة أو مفقودة أو مسروقة للحصول على معلومات العميل من المؤسسة المالية أو بشكل مباشر من عميل المؤسسة المالية.
 - أن يطلب من شخص آخر الحصول على معلومات عميل ما باستخدام بيانات كاذبة أو وهمية أو احتيالية أو باستخدام وثائق مزورة ووهمية ومخادعة أو وثائق مسروقة أو مفقودة أو مزيفة.
- تؤدي مثل تلك الادعاءات الاحتياطية إلى نوع جديد من المخاطر المتعلقة بالأمن والخصوصية، أو يمكن القول بأنها ستعرضنا إلى ما يعرف بسرقة الهوية Identity Theft. ويحدث هذا عندما يقوم شخص ما بسرقة المعلومات التعريفية الشخصية الخاصة بك لفتح حسابات سداد جديدة أو لطلب سلع ومنتجات أو للقيام باقتراض الأموال. وعادة لا يكتشف هؤلاء الضحايا المستهدفون من قبل لصوص الهويات الشخصية بأنهم ضحايا حتى يعجز هؤلاء السارقون عن دفع فواتير أو سداد قروض وتبدأ جهات التحصيل بمطالبة الضحايا المستهدفين بتسديد الحسابات التي لا علم لهم بها أصلاً. ووفقاً لهيئة التجارة الفيدرالية FTC فإن النماذج الأكثر شيوعاً في سرقة الهويات هي:
- الاحتيال على بطاقات الائتمان: فتح حساب بطاقة ائتمان باسم مستهلك ما أو الاستيلاء على حساب بطاقة ائتمان موجود بالفعل.
 - الاحتيال في خدمات الاتصالات: يقوم سارق الهوية بطلب خدمة هاتف أو هاتف نقال أو غيرها باسم المستهلك.
 - الاحتيالات البنكية: فتح حساب سواء كان جارياً أم ادخارياً باسم مستهلك ما وكتابة شيكات مزورة.
 - القروض الاحتياطية: يقوم سارق الهوية بطلب قرض ما كقرض شراء سيارة مثلاً باسم مستهلك آخر.

هناك قانون اتحادي مستقل مرتبط بقانون GLBA ألا وهو قانون منع سرقة الهوية والادعاءات الواهية The Identity Theft and Assumption Deterrence Act ، والذي اعتبر بأنه يعد جريمة فيدرالية أن يقوم شخص ما بشكل متعمد وبدون أي سلطة قانونية

بنقل أو باستخدام الوسائل التعريفية الخاصة بشخص آخر بقصد ارتكاب نشاط غير قانوني أو التحريض عليه، وأن ذلك يشكل انتهاكاً للقانون الفيدرالي، ويعتبر أيضاً جناية وفقاً لأي قانون يمكن تطبيقه على مستوى الولاية أو محلياً. يعد كل من الاسم أو رقم الضمان الاجتماعي "وسائل تعريفية"، وكذلك الأمر بالنسبة لرقم البطاقة الائتمانية أو الرقم التسلسلي الإلكتروني للهاتف الخليوي أو أي جزء آخر لمعلومات قد تستخدم بمفردها أو بالاشتراك مع غيرها من المعلومات لتحديد هوية شخص محدد.

قانون GLBA هو أحد القوانين التي بمقدورها التأثير على العديد من كبار المديرين، خاصة هؤلاء الذين يعملون في المؤسسات المالية على اختلاف أنواعها. وحيث إن العديد من جوانب قانون GLBA تهدف بالمقام الأول إلى حماية المعلومات المالية للعملاء، فقد أصبح الأمر الدارج إلى حد كبير هو أنه من المحتمل أن يكون لقانون GLBA آثار على مجموعة كبيرة من المؤسسات في الولايات المتحدة. لذا يجب على المؤسسات المالية والمناحة للائتمان أن تكون أكثر إدراكاً لقواعد قانون GLBA وقواعد الخصوصية العامة التابعة له والتي يمكن تطبيقها على العديد من المؤسسات الأخرى. وتعتبر شبكة الويب هي المصدر الأفضل بشكل مطلق للحصول على معلومات إضافية تفصيلية وحديثة عن قانون GLBA وأحكامه. وهناك مصدران جيدان لهذا الغرض هما:

١- لجنة التجارة الاتحادية: يقدم هذا المصدر الحكومي نظرة عامة على قانون GLBA ومعظم قواعده الحالية. على الرابط التالي:

<http://business.ftc.gov/privacy-andsecurity/gramm-leach-bliley-act>

٢- الجمعية الوطنية لمفوضي التأمين: وهي مؤسسة تنظيمية توجد في كل ولاية على حدة، حيث تمتلك كل مؤسسة من هذه المؤسسات التنظيمية معلومات عامة عن قانون GLBA يمكن الاطلاع عليها عن طريق زيارة الموقع www.naic.org، هذا بالإضافة إلى العديد من مواقع الويب الأخرى التي تغطي مواضيع ذات صلة بشكل تفصيلي.

على الرغم من أن قانون GLBA لا يزال أحد العناصر الهامة في تشريعات الولايات المتحدة، فإنه ظل إلى حد ما بعيداً عن الأنظار منذ عام ٢٠١١ في ظل المتطلبات المعقدة لما يعرف بقانون دود فرانك Dodd-Frank. حيث يعمل هذا القانون على تنفيذ التغيرات

التي، من جملة أمور أخرى، تؤثر في العمليات الرقابية والإشرافية على المؤسسات المالية، وتقدم أيضاً إجراءات حازمة جديدة للشركات المالية الكبرى، وإنشاء وكالة جديدة مسؤولة عن تنفيذ وفرض الامتثال للقوانين المالية التي تخص المستهلك، وطرح متطلبات رأسمالية تنظيمية أكثر قوة، والمساهمة في إحداث تغيرات كبيرة وهامة في اللائحة التنظيمية لما يسمى بالمشتقات المالية، وتعديل اللوائح التنظيمية الخاصة بوكالات التصنيف أو التقييم الائتماني، وإحداث تغيرات على حوكمة الشركات والممارسات التنفيذية للتعويضات، واشتراط تسجيل المستشارين للحصول على تمويل خاص، والمساهمة أيضاً في إحداث تغيرات كبيرة في سوق التورق. أي أنه بمعنى آخر، يمكن القول إن هذا القانون قد أحدث الكثير من الأمور والتغيرات.

يعتبر هذا القانون واحداً من العناصر المعقدة في التشريع وقد تمت صياغة المسودة الخاصة ببنود هذا القانون في الوقت الذي كان فيه هذا الكتاب تحت الطابعة. ومن خلال استطلاعنا المحدود على هذا التشريع، تبين أن لهذا القانون بعض الاهتمامات المباشرة في حوكمة تقنية المعلومات. في جميع الأحوال يعد هذا القانون عنصراً آخر من عناصر التشريع التي أسهمت في وضع قواعد جديدة للعديد من المؤسسات هذه الأيام.

قانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة (HIPAA): العناية الصحية وأكثر:

سيُطلب من المدير المقيم في الولايات المتحدة الذي يقوم بزيارة الطبيب هذه الأيام لإجراء الفحوصات السنوية أو لأي إجراءات أخرى أن يوقع على ما يشبه موافقة خطية تهدف إلى السماح بالإفصاح عن معلوماته، وذلك قبل الشروع في عمل الفحوصات، وذلك أثناء قيامه بإجراءات حجز الكشف عند وصوله مكتب الاستقبال. حيث يتم بموجب هذه الوثائق الحصول على موافقة المريض أو المريضة على السماح بمشاركة السجلات الطبية الخاصة به أو بها أو الإفصاح عنها على أنها جزء من الإجراءات الخاصة بهذه الزيارة الطبية. وإذا قام هذا المدير المريض بالسؤال عن سبب ذلك الإجراء، تكون الإجابة غالباً بأن هذا الإجراء هو "أحد المتطلبات القانونية الخاصة بقانون HIPAA". ويكون رد الفعل الطبيعي للمريض عادة هو القيام بالتوقيع على تلك الوثائق المطلوبة والاستمرار بالإجراءات دون أن يكون هناك فهم تام للغاية الحقيقية من الحصول على هذا التوقيع. فعلى الرغم من

مجموعة القواعد الخاصة بالعناية الصحية الواردة في قانون HIPAA، فإنه يحتوي أيضاً على قواعد تشريعية أخرى تتعلق بالخصوصية، تذهب إلى ما هو أبعد من العناية الصحية، وسوف تؤثر في العديد من المؤسسات وكذلك المدققين الداخليين التابعين لها.

يتطلب العمل في الولايات المتحدة الأمريكية سواء كان ذلك في شركة صناعية أو مؤسسة خدمات مالية أو الكثير غيرها، أن يكون لدى كبار المديرين مستوى فهم وإدراك عام لقانون HIPAA وقواعده. فقد صدر هذا القانون عام ١٩٩٩م، وتم إصدار القواعد النهائية له خلال السنوات اللاحقة لتلك السنة. وقد كان لقانون HIPAA أثر كبير في الولايات المتحدة الأمريكية في خصوصية وأمن معلومات السجلات الطبية الشخصية وعلى العديد من السجلات الشخصية الأخرى. يتعرض الأفراد لقانون HIPAA عند قيامهم بزيارة إحدى العيادات الطبية الخاصة بأحد الأطباء أو عند تعرضهم للعديد من المسائل الطبية الأخرى المتعلقة بالأمور الطبية. كما تشهد أيضاً إدارات الموارد البشرية في المؤسسات أثر ونتائج متطلبات قانون HIPAA هذه الأيام على إدارتها لسجلات مخططات الرعاية الصحية والمعالجات الطبية الخاصة بالموظفين لديها. ومن المؤكد أن هذا القانون قد تسبب أيضاً في إحداث آثار كبيرة ومتزايدة وبدرجة غير مسبقة على مجمل قطاع الرعاية الصحية وعلى جميع مقدمي خدمات الرعاية الصحية التابعين له. والأهم من هذا كله أن قواعد هذا القانون قد شملت مجموعة كبيرة من عمليات الأعمال القائمة على التجارة الإلكترونية.

لهذا القانون التشريعي الأساسي أربعة أهداف:

١- التأكيد على إمكانية نقل التأمين الصحي من خلال إزالة القيود والشروط الوظيفية التي كانت موجودة في السابق. وقد كان ذلك بمثابة المحفز الرئيسي الذي أدى إلى إقرار قانون HIPAA. حيث كان في السابق يتم إجراء العمليات التشخيصية والفحوصات اللازمة للأشخاص في ظروف وتحت شروط معينة، ولكن بعد ذلك كان أغلب هؤلاء الأشخاص لا يستطيعون الحصول على تغطيات صحية جديدة عند قيامهم بتغيير الجهات التي يعملون بها، وذلك لأن عملية مشاركة المعلومات المتعلقة بتلك الحالات الصحية الخاصة بهؤلاء الأشخاص مع الآخرين كانت في كثير من الأحيان تتم بشكل غير مرن.

٢- الحد من عمليات الغش والاحتيال وسوء المعاملة في كل ما يتعلق بأمور الرعاية الصحية. فقد أدت تلك الكلمات التي تم طرحها في جلسات الاستماع الخاصة داخل الكونجرس الأمريكي عندما تم الاستشهاد ببعض الأمثلة عن الاحتيال وسوء المعاملة المزعومة إلى تشريع هذا القانون.

٣- فرض معايير خاصة بالمعلومات الصحية. وقد تم تغطية ذلك من خلال قواعد الخصوصية والأمن الواردة في قانون HIPAA والتي سنوجزها لاحقاً.

٤- ضمان أمن وخصوصية المعلومات الصحية.

سيقدم هذا القسم نظرة عامة وموجزة عن أهداف قانون HIPAA والقواعد الناتجة عنه، والتي تغطي مسائل حوكمة وخصوصية وأمن تقنية المعلومات. وعلى الرغم من عدم طرح جميع الجوانب والقضايا المتعلقة بقانون HIPAA في هذا الكتاب، فإننا نتحدث عنه هنا على أنه قانون تشريعي آخر تقوده "القواعد الجديدة" التي لا تزال تؤثر في العديد من كبار المديرين في المؤسسات. إن التقدم الذي حدث في هذا القانون التشريعي يوضح ويفسر آليات العمل المتبعة لوضع وإقرار القوانين التي تتم تحت رعاية وإشراف الجهات الحكومية المعنية. في البداية، كان الإصدار الأول لقواعد قانون HIPAA على شكل مسودة تابعة لأحد اللوائح التي كانت قد نشرت في وقت مبكر. وقد كان هناك العديد من الملاحظات والتعليقات الموجودة على تلك المسودات، وكان لا يزال هناك المزيد من الملاحظات والتعليقات على مسودات لقواعد منقحة ومحسنة تم إصدارها لاحقاً، وقد تم إصدار نسخ القواعد الأخيرة الخاصة بهذا القانون في وقت متأخر جداً عما كان مخطط له في الأصل.

قواعد الخصوصية لسجلات المرضى وفقاً لقانون HIPAA:

كانت الاهتمامات والمخاوف المستمرة المتعلقة بمسائل الخصوصية الطبية للمرضى من الأسباب التحفيزية الرئيسية التي جعلت الكونجرس الأمريكي يوافق على إقرار قانون HIPAA. فعندما نقوم بزيارة إحدى المراكز المتخصصة بتقديم خدمات الرعاية الطبية، لمناقشة بعض المخاوف أو مشكلة ما، فإننا نتوقع بعد ذلك أن تتم المعالجة بطريقة سرية وخاصة للغاية. فنحن لا نرغب مثلاً في أن يتم إرسال النتائج الخاصة بالزيارات التي قمنا

بها للمراكز والعيادات الطبية إلى إدارة الموارد البشرية التابعة للأماكن التي نعمل بها، أو أن يتم إرسال تلك النتائج لإحدى شركات التأمين التي لا تربطها أي علاقة بالموضوع وليست بحاجة لمعرفة تلك النتائج، أو أن يتم ترك تلك النتائج على أحد مكاتب الاستقبال الخاصة بمقدمي الخدمات الطبية ليقوم بعد ذلك شخص ما بالتقاطها والتصرف فيها بكل سهولة. والأسوأ من هذا كله، هو أننا لا نرغب في أن تتم مشاركة تلك النتائج أو المعلومات أو أي مسائل شخصية وسرية بصورة قد تحد من فرص وخيارات التوظيف المستقبلية الخاصة بنا. هذا الخوف أو القلق المرتبط بمسألة خصوصية المعلومات الشخصية، هو السبب الأساسي وراء العديد من قواعد قانون HIPAA. من ناحية أخرى، فهناك العديد من الأطراف التي ترغب في الحصول على معلومات تتعلق بشروط الرعاية الصحية لدينا لتقديم تغطية صحية وتعويضات مالية ملائمة، ومن الناحية العملية فإنه يمكننا القول بأن جميع العمليات التشغيلية الخاصة بتقديم خدمات الرعاية الصحية تحتاج إلى نظم داعمة تفصيلية ومعقدة جداً. وتغطي قواعد قانون HIPAA خمسة مجالات عامة سنتحدث عنها جميعاً بشكل موجز في الفقرات التالية. إن هذه الفقرات هنا لا تقدم تغطية شاملة لقواعد هذا القانون، وليس الغرض منها هو أن تكون مصدراً مرجعياً لتلك القواعد، وإنما تهدف إلى إعطاء المهنيين من خارج القطاع الطبي لمحة عامة عن القواعد الجديدة التالية الخاصة بقانون HIPAA.

١- استخدامات السجلات الطبية والإفصاح عنها: ينبغي على المؤسسة الخاضعة لقواعد قانون HIPAA أن تتخذ الخطوات اللازمة للحد من استخدام المعلومات الطبية الشخصية والإفصاح عنها ليكون ضمن "الحد الأدنى الذي لا بد منه لإنجاز وإتمام الغاية التي من أجلها تم استخدام تلك البيانات أو الإفصاح عنها أو طلبها" في القضايا والأمور غير العلاجية. وسنبدأ في طرح النظرة العامة عن قواعد قانون HIPAA بكلمات وعبارات مقتبسة بشكل مباشر من نصوص تلك القواعد، كاستخدام عبارة "the minimum necessary" بمعنى "الحد الأدنى اللازم" في الجملة السابقة. حيث يحتوي القانون على العديد من الأمثلة الخاصة بهذه الإرشادات التوجيهية المتعلقة بالممارسات التي تختارها المؤسسة لكي تتحقق من مدى صحتها من خلال الاطلاع على أحكام وتداعيات أخرى سابقة كانت قد وقعت على مر السنين.

جاء هذا القسم من قواعد قانون HIPAA لتوضيح أن المعلومات الصحية الشخصية الخاصة بشخص ما ستفقد حماية هذا القانون HIPAA لها في حال كان هناك نقص في المعلومات الخاصة بهذا الشخص المعني بهذا القانون، كعدم احتواء تلك المعلومات الصحية على أي من المحددات أو المعلومات الثمانية عشر الخاصة بمعلومات حول هذا الشخص وعلاقاته أو علاقاتها وأصحاب العمل وأفراد أسرته أو أسرته. إن هذا المطلب يقول الكثير عن قانون HIPAA. فلتحقيق الامتثال لنظام المعلومات الصحية الخاص بقانون HIPAA، قام هذا القانون التشريعي بتحديد تلك الثمانية عشر معاملاً التي يجب أن يستخدمها أي أخصائي تقنية معلومات أثناء قيامه بتنفيذ عمليات استرجاع البيانات من قاعدة البيانات بهدف تحديد هوية شخص ما. هذا يعني، أنه سواء كانت المعلومات الطبية الخاصة بشخص ما موجودة في ملف أو في نظام معلوماتي محمي ضد عمليات الإفصاح العام للآخرين، فإنه من الممكن مشاركة تلك المعلومات مع الآخرين في ظروف وشروط معينة.

٢- متطلبات التفويض أو التصريح: هذا القسم في HIPAA هو الذي يتعرض له معظم مستخدمي خدمات الرعاية الصحية. لذا يجب أن يحصل مقدمو خدمات الرعاية الصحية على موافقة خطية تتعلق بالسماح لهم بالإفصاح عن جميع المعلومات الخاصة بالرعاية الصحية باستثناء بعض حالات الطوارئ. وللشخص الحق في عدم الموافقة على مثل هذا الأمر الذي يتعلق بالإفصاح أو الكشف عن معلوماته الطبية، وهناك شرط حاسم وقوي يفرض على مقدمي خدمات الرعاية الصحية القيام بالاحتفاظ بالسجلات الضرورية للقيام بتتبع جميع العمليات المتعلقة بهذه الإفصاحات. وكما ذكرنا سابقاً، فإن هذا هو ما يُطلب من الشخص التوقيع عليه عند قيامه بزيارة أحد المراكز أو العيادات الطبية من خلال تقديم مجموعة من الوثائق التي تحتاج إلى توقيعه.

٣- نشر الممارسات المتعلقة بالخصوصية: يجب أن يكون لدى مقدمي خدمات الرعاية الصحية ممارسات وإجراءات منشورة للخصوصية التي ينبغي عليهم توفيرها لمستخدمي المستفيدين من خدمات الرعاية الصحية المقدمة. بعد ذلك يحق للأفراد أن يطلبوا بشكل رسمي المزيد من القيود والمحددات التي يرغبون فيها على تلك السياسات المتبعة، ويجب على مقدمي الخدمات الصحية استيعاب جميع الطلبات المعقولة والمنطقية للمستخدمين.

٤- حقوق الوصول للسجلات الطبية والتعديل عليها: للأشخاص الحق في فحص أو نسخ (جزئي أو كلي) للمعلومات الصحية الشخصية الخاصة بهم. كما أن لديهم الحق في طلب إجراء تعديلات مناسبة على تلك السجلات الصحية الخاصة بهم. كما يجب أن يقوم مقدمو الرعاية الصحية بالاحتفاظ بسجلات عن جميع الأطراف التي طلبت الوصول إلى تلك السجلات الشخصية للمعلومات الصحية الخاصة بهم خلال الشهور الستة الأخيرة.

٥- إدار الخصوصية في قانون HIPAA: بالذهاب إلى ما هو أبعد من قواعد الوصول للسجلات والإفصاح عنها، فإن لدى قانون HIPAA مجموعة واسعة من المتطلبات المتعلقة بإدارة الخصوصية. ويتم تطبيق هذه المتطلبات أو القواعد على ما يعرف بالكيانات المشمولة "Covered Entities" كالعيادات الطبية والمختبرات والمستشفيات وكل ما له علاقة بأمور الرعاية الصحية الشخصية. وتشتمل القواعد الخاصة بإدارة الخصوصية على ما يلي:

- ينبغي على مقدم خدمات الرعاية الصحية تعيين "موظف خصوصية Privacy Official" يكون مسؤولاً عن الأمور المتعلقة بالخصوصية، بحيث يكون هو المعني بقضايا تطوير وتطبيق تلك الإجراءات والسياسات الخاصة بقانون HIPAA.

- ينبغي على مقدم خدمات الرعاية الصحية أن يقوم بتدريب أعضاء كادر العمل أو الموظفين لديه على التعاطي مع سياسات وإجراءات قانون HIPAA المتعلقة بالخصوصية، كما يجب عليه الاحتفاظ بالوثائق التي تثبت بأن هذه التدريبات قد تمت فعلاً.

- ينبغي على مقدم خدمات الرعاية الصحية أن يمتلك ضمانات وتدابير أمنية، وإدارية، وفنية، ومادية معمولاً بها لحماية خصوصية المعلومات الصحية الشخصية.

- ينبغي على مقدم خدمات الرعاية الصحية تطبيق "العقوبات المناسبة Appropriate sanctions" على الموظفين غير الملتزمين بتلك الإجراءات والسياسات المتعلقة بالخصوصية.

- ينبغي على مقدم خدمات الرعاية الصحية إيجاد وتطبيق السياسات والإجراءات المصممة لتحقيق الامتثال أو الامتثال لعناصر موجودة في اللوائح التنظيمية الخاصة بقانون HIPAA. كما يجب الاحتفاظ بتلك الوثائق الرسمية لمدة ستة أعوام، سواء كانت مكتوبة على أوراق أم على شكل نماذج إلكترونية.

وعلى الرغم من أن تلك القواعد الخاصة بقانون HIPAA تشمل بالمقام الأول عمليات الوصول للمعلومات الصحية الشخصية، فإنها ذكرت مجالات أخرى تحدد ممارسات تشغيل جيدة يجب أن يتم تطبيقها في أي مكان آخر في داخل المؤسسة. والمثال على ذلك هو تضمينها لشرط الاحتفاظ بالوثائق المتعلقة بالبرامج التدريبية التي تم إنجازها من قبل مقدمي خدمات الرعاية الصحية. فقد تم وضع هذا النوع من القواعد أو المطالب في البداية للبرامج الطبية للإدارة الاتحادية للعقاقير أو برامج الدواء. أما الآن فإن هذه القواعد تمثل جزءاً أساسياً من قانون HIPAA وتعتبر فكرة جيدة بالنسبة لمعظم البرامج التدريبية في الشركات. فالمؤسسات في بعض الأحيان تنفق الكثير من مواردها الخاصة في تدريب موظفيها إلا أنها لا تكلف نفسها غالباً عناء القيام بتوثيق هذا النشاط التدريبي على نحو جيد.

إن لهذه القواعد وغيرها من القواعد المذكورة في هذا الفصل أهمية خاصة بالنسبة للمسؤول التنفيذي الذي يعمل في إحدى المؤسسات التي لها علاقة بالمسائل المتعلقة بالرعاية الصحية كالمستشفيات أو شركات التأمين الطبي. فضلاً عن أن هذه القواعد تتسع وتمتد لتصل إلى مجالات أخرى مثل معالجة المطالبات الخاصة بالتأمين الطبي في إدارة الموارد البشرية لإحدى المؤسسات، أو المتعلقة بسلامة مرافق المصنع والتبليغ عن الحوادث الصناعية. يجب أن يكون لدى جميع المؤسسات المعنية بقضايا الرعاية الصحية أيضاً قواعد وإجراءات امتثال قوية لقانون HIPAA، إلا أن تقديم وصف تفصيلي لمثل هذه القواعد والإجراءات المتبعة ليس من ضمن نطاق وأهداف هذا الكتاب. على كل حال فإن الامتثال لقانون HIPAA يعد أيضاً مطلباً في العديد من البيئات الأخرى. يوضح الشكل التوضيحي (٣-١١) بعض إجراءات حوكمة تقنية المعلومات فيما يخص قانون HIPAA التي يجب أن تكون موجودة ومفعلة في أي مؤسسة خاضعة لقانون HIPAA.

التشفير ومتطلبات الأمن في قانون HIPAA:

بالإضافة إلى قواعد الخصوصية المتعلقة بالتفويض والإفصاح عن السجلات الطبية، فإن قانون HIPAA يحتوي أيضاً على بعض متطلبات أمن تقنية المعلومات التي تم تحديدها بدقة والتي يصعب تطبيقها في العديد من المؤسسات الصغيرة. فهو يدفع على حدود الممارسات الأمنية لتقنية المعلومات (زيادة حجم الممارسات الأمنية التقنية) بالنسبة

للعديد ويحتاج بعض الأمور كالقيام بتأمين التوقيعات الإلكترونية على الرغم من محدودية التقنيات الناضجة أو الفعالة فنياً المستخدمة حالياً لتوفير مثل هذه التوقيعات الإلكترونية الآمنة في ظل وجود الشبكات المفتوحة كشبكة الإنترنت. فنحن لا زلنا في المرحلة التي قد يتمكن فيها أحد القراصنة المهرة لنظم الحاسبات من اعتراض أو اختراق إحدى مكالمات الهاتف الخليوي التي تتناول بعض المواضيع والمسائل المتعلقة بالمعلومات الخاصة بالرعاية الصحية، الأمر الذي يعتبر بمثابة اختراق لمتطلبات الأمن والسرية لقانون HIPAA. ستتغير التقنية في المستقبل وستتحسن إجراءات الضبط والرقابة وسيزداد ذكاء وخبرة القراصنة وسيتم تسوية هذه الاختراقات والانتهاكات في المحاكم.

لقد كان السبب الرئيسي وراء وضع مثل تلك القواعد السرية هو عدم ملاءمة وكفاية العديد من نظم إدارة تقنية المعلومات الخاصة بالرعاية الصحية التي كانت موجودة قبل قانون HIPAA. ففي كثير من الأحيان نرى أن المؤسسات يمكنها تحسين هذه النظم الأمنية لا عن طريق شراء وتركيب برمجيات جديدة فحسب، بل عن طريق تحسين السياسات التي يقودها البشر أولاً. وقد تم الانتهاء من قواعد المعايير الأمنية الخاصة بقانون HIPAA ووضعها حيز التنفيذ في شهر إبريل من عام ٢٠٠٣. إلا أنه لم يتم تفعيل معايير الامتثال لتلك القواعد حتى عام ٢٠٠٦. ومن بين المجالات الأخرى التي تشملها هذه القواعد ما يُطلق عليه قانون HIPAA اسم "الوحدات المشمولة Covered Entities" والتي تشمل:

- الأطباء وغيرهم من الذين يقومون بتقديم خدمات الرعاية الصحية والذين يقومون بمعالجة مطالبات الرعاية الصحية بشكل إلكتروني.
- الخطط الصحية بما فيها مؤسسات التأمين الذاتي.
- دور المقاصة الخاصة بالخدمات الصحية - لخدمات الفواتير وغيرها والذين يقدمون خدمات تهيئة البيانات الخاصة بالمطالبات الإلكترونية المقدمة.

شكل توضيحي (٣-١١)

المتطلبات والإجراءات الخاصة بحوكمة تقنية المعلومات في قانون HIPAA.

١. يجب أن يتم تعريف المؤسسة على أنها أحد المؤسسات المعنية بتقديم خدمات الرعاية الصحية والخاضعة لقانون HIPAA. (إن كان هذا غير متوفر، فليس هناك حاجة لاستكمال باقي الخطوات).
٢. للامتثال لقانون HIPAA وللخطة التنفيذية العامة لموضوعه لهذا القانون، فلا بد من تعيين موظف رسمي مسؤول عن أمن المعلومات المتوفرة على مستوى المؤسسة.
٣. لا بد من وضع وتنفيذ سياسات وإجراءات لحماية المعلومات الصحية الخاصة بالمرضى.
٤. يجب أن يكون هناك عمليات معمول بها للقيام بعمليات الدعم والرقابة المستمرين لقواعد قانون HIPAA ولوائحها.
٥. يجب أن تتضمن عمليات قانون HIPAA سياسات وإجراءات وضوابط وتقنيات شاملة فيما يتعلق بمسائل الخصوصية والأمن.
٦. لا بد أن يكون للمؤسسة خطة رسمية للطوارئ معمول بها تتضمن ما يلي: <ul style="list-style-type: none"> • التحليلات الحساسة للتطبيقات والبيانات. • خطط النسخ الاحتياطي للبيانات. • خطط التعافي من الكوارث Disaster Recovery. • خطة للعمليات التشغيلية خلال حالة الطوارئ. • الفحص والتنقيحات الدورية المقترحة للخطة.
٧. يجب أن تشمل عمليات قانون HIPAA على عمليات رسمية لضبط الوصول إلى البيانات، والتي تتضمن أيضاً العمليات المتبعة للحصول على إذن الوصول للبيانات وقواعد إنشاء الاتصال بالبيانات والإجراءات اللازمة لتعديل الوصول إلى البيانات.
٨. يجب أن تشمل الضوابط الموضوعية لمراقبة عمليات الوصول إلى الوسائط الخاصة بنظم المعلومات على العمليات التالية: <ul style="list-style-type: none"> • المساءلة. • نسخ احتياطية للبيانات. • تخزين البيانات. • التخلص من البيانات.

٩. يجب على الإجراءات أو السياسات الأمنية الشخصية أن:
<ul style="list-style-type: none">• تضمن الإشراف على موظفي الصيانة من قبل شخص مطلع ومفوض بذلك.• تحتفظ بسجلات كاملة عن التصريح بالوصول للمعلومات.• تضمن حصول موظفي التشغيل والصيانة على تفويض أو إذن وصول مناسب.• توفير إجراءات إجازة الموظفين .
١٠. يجب أن يكون هناك إجراءات رسمية معمول بها لإنهاء الخدمات، والتي تتضمن تغيير مجموعة مناسبة من الأقفال والإزالة من قوائم الوصول أو الحصول على البيانات.
١١. يجب أن تشتمل ضوابط الوصول الفعلي للنظم والمعلومات في جميع أنحاء المؤسسة على:
<ul style="list-style-type: none">• خطط عمليات التشغيل في حالة الطوارئ.• مراقبة وضبط المعدات داخل وخارج المنشأة.• خطط أمن المرافق.• إجراءات التحقق من تصاريح الوصول قبل الوصول الفعلي إلى النظم والبيانات.• سجلات الصيانة.• الإجراءات اللازمة لمعرفة عمليات الوصول للنظم والبيانات بالنسبة للذين يصرح لهم ذلك.• تسجيل الدخول للزوار والمرافقين إذا كان ذلك مناسباً.• فحص وتنقيح خطة الوصول الفعلي للبيانات.
١٢. يجب حماية جميع الشبكات والاتصالات من خلال:
<ul style="list-style-type: none">• الخروج التلقائي.• الهوية الفريدة للمستخدم.• كلمات المرور وأرقام التعريف الشخصية PINs.• أنظمة الرد الهاتفية.

يعني ذلك أن قواعد الأمن والسرية الموجودة في قانون HIPAA يتم تطبيقها على جميع المؤسسات، سواء كانت عبارة عن عيادة يوجد بها طبيب واحد أم مستشفى كبيراً أو مكتباً صغيراً متخصصاً في معالجة المطالبات الخاصة بقضايا الرعاية الصحية التابعة لها من خلال التأمين الذاتي.

قواعد الأمن والسرية هي العنصر الرئيسي في قانون HIPAA المعني بالحفاظ على خصوصية المعلومات الصحية الشخصية. وتغطي هذه القواعد ممارسات جيدة فيما يتعلق بالأمن والسرية لما هو أكثر بكثير من مجرد حماية للسجلات الطبية، كالمطالبات الخاصة بالمعايير القوية للتعافي من الكوارث. تحتوي القواعد المنشورة لقانون HIPAA على نوعين من القواعد هما: قواعد مطلوبة أو إلزامية "Required" وقواعد غير إلزامية "Addressable" كما أطلق عليها القانون. هذا النوع الأخير يمثل القواعد التي لا يُطلب من المؤسسة القيام بتنفيذها أو تطبيقها نظراً لصغر حجمها أو قلة مواردها. أما القواعد الإلزامية لقانون HIPAA فتمثل العديد من الممارسات الجيدة في مجال أمن المعلومات التي تناسب جميع المؤسسات. هناك مجالات أمن أخرى في قانون HIPAA لكنها خارج نطاق وأهداف هذا الكتاب، كالمطالبات الخاصة في بيئة البنية التحتية الرئيسية العامة والتي تتضمن التوقيعات الرقمية.

الإجراءات الإدارية الأمنية لتقنية المعلومات في قانون HIPAA:

يحتاج قانون HIPAA إلى إجراءات إدارية معمول بها لحماية سلامة البيانات وخصوصيتها وإتاحتها. ويجب أن يتم توثيق هذه الإجراءات بحرص وعناية لكل قاعدة من قواعد قانون HIPAA. يعرض الشكل التوضيحي (١١-٤) بعض هذه الإجراءات الإدارية الإلزامية "Required". كما يوضح هذا الشكل أيضاً القواعد التنفيذية لكن بطريقة عامة جداً، أما بالنسبة للقواعد المنشورة لقانون HIPAA فقد جاءت بشكل أكثر تفصيلاً. إن العديد من هذه المتطلبات كخطة الطوارئ الموثقة والمختبرة أو السياسات الرسمية لضوابط الوصول للمعلومات، تكون مشابهة لإجراءات الضبط والرقابة التي أوصى بها المدققون الداخليون على مر السنين. بعضها يمثل الممارسات الجيدة في حوكمة تقنية المعلومات التي ينبغي أن تكون معمولاً بها في العديد من المؤسسات. على سبيل المثال، يشير الشرط رقم ٣

في الشكل التوضيحي (١١-٤) إلى الحاجة إلى ما يسمى سياسة العقوبات - وهي مجموعة رسمية من القواعد التي تُطبق على الأشخاص الذين يخترقون سياسة الأمن. إنها لفكرة جيدة بالنسبة إلى معظم المؤسسات هذه الأيام، وكقاعدة إدارية، أن يتعرض مقدم خدمات الرعاية الصحية الخاضع لقانون HIPAA للجزاءات إذا تم اكتشاف عدم ملاءمة وكفاءة القواعد والإجراءات المتبعة لديه.

وتشتمل المتطلبات الأمنية لقانون HIPAA أيضاً على القواعد الوقائية المادية المشابهة لضوابط الوصول الفعلي للبيانات التي كانت موجودة على مراكز البيانات الخاصة بتقنية المعلومات والتي تعود إلى الأيام الأولى لأجهزة الحاسبات المركزية الضخمة mainframe. في جميع الأحوال، استطاع قانون HIPAA هنا أن يتخطى حدود مركز عمليات التشغيل التقليدي لتقنية المعلومات، ويدعو إلى إيجاد إرشادات توجيهية ووثائق قوية تتعلق باستخدام محطة العمل والموقع. وعلى الرغم من أنه قد جرت العادة ألا تقوم إدارة تقنية المعلومات ومدققوها الداخليون بإثارة العديد من المخاوف لدى الرقابة الداخلية التي تتعلق بالضوابط المادية للأجهزة الطرفية المتصلة من خلال الربط الشبكي في البيئة الخاصة بمنشأة الأعمال، إلا أن بيانات العناية الصحية الخاضعة لتنظيم قانون HIPAA تطرح العديد من القضايا الجديدة. فقد تكون محطة عمل البيئة الطبية التي ربما يكون فيها أطباء وممرضون وغيرهم من الموظفين، بحاجة إلى ضوابط منطقية ومادية قوية لحماية الخصوصية الشخصية لسجلات المرضى التي يمكن أن يتم تسريبها من خلال تلك المحطات.

شكل توضيحي (١١-٤)

المواصفات المطلوبة لتطبيق قانون HIPAA

أحكام للوحدات المشمولة "Covered" كجزء من خطة الأمن والامتثال لقانون HIPAA.
١. تحليل المخاطر: يجب على المؤسسات إجراء تقييم أو تقدير كامل للمخاطر المحتملة المتعلقة بسرية وسلامة وإتاحة البيانات.
٢. إدارة المخاطر: يجب على المؤسسات المشمولة تطبيق تدابير أمنية ملائمة ومعقولة للحد من المخاطر وإبقائها ضمن المستوى المقبول (لتكون تحت السيطرة).
٣. سياسة العقوبات: لا بد من تطبيق العقوبات والجزاءات على أعضاء الكادر الوظيفي الذين يخترقون السياسات الأمنية المتعلقة بالخصوصية في المؤسسة، كتطبيق سياسة من نوع "ثلاثة أخطاء، إذا أنت مطرود من العمل" (وهي السياسة التي تفرض المزيد من العقوبات على هؤلاء الأشخاص الذين يدانون بجريمة خطيرة علماً أنهم كانوا قد أدينوا سابقاً باثنتين من القضايا الخطيرة أيضاً).
٤. الإبلاغ عن إعداد تقارير بشأن نشاط أمن نظم المعلومات: لا بد من التبليغ عن سجلات أمن المعلومات وتقارير الحوادث وغيرها من التقارير المتعلقة بالأنشطة الأمنية والقيام بمراجعتها بشكل منتظم.
٥. إجراءات الاستجابة للحوادث: لا بد من وجود عمليات معمول بها لتحديد الحوادث الأمنية والتحقيق فيها والتخفيف من آثارها وتوثيقها.
٦. إجراءات النسخ الاحتياطي: لا بد من وجود إجراءات معمول بها للتعافي من أي خسارة أو فقدان للبيانات.
٧. التعافي من الكوارث: ينبغي على كل مؤسسة مشمولة بالقانون أن تقوم بوضع الإجراءات المناسبة التي تغطي أي فقد للبيانات.
٨. حالة الطوارئ الخاصة بعمليات التشغيل: لا بد من وجود عمليات معمول بها لضمان أمن وسرية معلومات المرضى عندما يكون التشغيل في حالة الطوارئ.
٩. العقود التجارية ذات العلاقة. يجب على المؤسسة تضمين أسلوب في عقود الموردين يشترط على المورد تبني تدابير أمنية كافية للإبلاغ عن الحوادث الأمنية التي تقع في المؤسسة وضمان تطبيق المقاولين الفرعيين (مقاولي الباطن) للتدابير الأمنية الملائمة وفسخ العقد في حال تبين وجود أي اختراقات أمنية.
١٠. التخلص من معلومات المريض: لا بد من وجود سياسات وإجراءات معمول بها لمعالجة الأرشفة النهائية لمعلومات المريض وحفظها.

١١. إعادة استخدام الوسائط: لا بد من توفير العمليات المعمول بها لضمان إزالة المعلومات الحساسة من الوسائط الإلكترونية كمشغلات الأقراص قبل القيام بإعادة استخدامها.
١٢. معرف فريد لهوية المستخدم: يجب تخصيص محددات أو معرفات فريدة لجميع مستخدمي النظم لمنع مشاركة الحسابات ولتتبع سلوك النظام.
١٣. إجراءات الوصول للبيانات في حالة الطوارئ: لا بد من إيجاد إجراءات تسمح بالوصول إلى المعلومات الإلكترونية في حالات الطوارئ.
١٤. التوثيق: لا بد من إيجاد إجراءات لضمان أمن وسرية المعلومات والحفاظ على الوثائق لمدة ست سنوات ومراجعتها بشكل دوري.

الخدمات والآليات الخاصة بالأمن التقني:

تتطلب قواعد قانون HIPAA وجود عمليات معمول بها لحماية سلامة وسرية وإتاحة بيانات السجلات الطبية ومنع الوصول غير المصرح به لأي من البيانات المرسلّة عبر شبكات الاتصال المستخدمة. تحتاج هذه القواعد غالباً إلى ضوابط أكثر قوة وصرامة من تلك الموجودة في بعض المؤسسات الكبيرة. وتتضمن هذه الضوابط الأمور التالية:

- **ضوابط الوصول إلى البيانات:** لا بد من إيجاد آليات رقابية قوية تعتمد على سياق البيانات أو دور أو مركز المستخدمين المصرح لهم. هذا بالإضافة إلى العمليات الرقابية التي يجب دائماً أن تكون في موضع التنفيذ للسماح بالحصول على البيانات في حالات الطوارئ بواسطة العمليات التشغيلية لمركز البيانات إذا تطلب الأمر.

- **ضوابط التدقيق:** يوجد مطالبات هنا وفي جميع القواعد الأخرى لقانون HIPAA بضرورة وجود ضوابط تدقيق قوية، والتي تتضمن وجود أمور كعمليات التنقيح أو التعديل للتوثيق وعمليات مراقبة الآثار والمسارات التقليدية الخاصة بالتدقيق.

- **اعتماد صحة البيانات:** هناك حاجة إلى ضوابط نظم قوية لحماية وسلامة البيانات.

- **اعتماد الكيان:** لا بد من وجود ضوابط معمول بها بحيث أنه عندما تحاول إحدى محطات العمل الوصول إلى محطة عمل أخرى، فلا بد أن يكون مصرحاً لها القيام بذلك.

وقد تتضمن هذه العملية استخدام ضوابط لكلمات المرور أو الرد الآلي على الهاتف أو حتى ضوابط المقاييس الحيوية. لقد تخطى هذا المطلب حدود الكثير من ممارسات المؤسسات المطبقة هذه الأيام، حيث يتم مشاركة أو تبادل البيانات بكل سهولة وحرية من خلال رسالة البريد الإلكتروني ومرفقاتها.

• **ضوابط الاتصالات والشبكة:** هناك مجموعة واسعة من الضوابط المقترحة هنا مثل التنبيهات والتشفير والإبلاغ عن الأحداث والتصديق على الرسائل وغيرها. يجب على المؤسسة الخاضعة لقانون HIPAA أن تقوم بتنفيذ شبكة آمنة جداً.

يقتضي قانون HIPAA أن تمنح الضوابط الخاصة بالتوقيع الإلكتروني البيانات الموقعة إلكترونياً الوزن القانوني نفسه للمستندات الورقية التي وقع عليها توقيعاً تقليدياً. حيث ينص قانون HIPAA على سلامة الرسائل الشبكية وعدم إنكار واعتماد المستخدم لأي رسالة تحتوي على توقيع إلكتروني. وقد يشكل هذا تحدياً إضافياً بالنسبة للعديد من الأشخاص. وتستخدم اليوم عمليات التوقيع الرقمي أو الإلكتروني، إلا أنها مرهقة بعض الشيء ولن تكون إلزامية حتى يتم تطوير تقنيات جديدة أفضل لضمانها.

أسهمت قواعد قانون HIPAA في تقدم العديد من المجالات المتعلقة بأمن وسلامة تقنية المعلومات. وعلى الرغم من أن هذه القواعد قد وُجِدَت من أجل المؤسسات المعنية بتقديم خدمات الرعاية الصحية، فإنها ستؤثر في العديد من المؤسسات الأخرى. لذا يتعين على كبار المسؤولين التنفيذيين محاولة الحفاظ على مستوى عام من المعرفة الخاصة بتلك القواعد السارية ومعاييرها المطلوبة حتى وإن كانوا لا يعملون بشكل مباشر في إحدى مؤسسات تقديم خدمات الرعاية الصحية. وقد قمنا في هذا الفصل بتقديم نبذة مختصرة جداً عن تلك القواعد المعقدة والهامة في الوقت نفسه. وبالذهاب إلى ما هو أبعد من مجرد مؤسسات الرعاية الصحية، فإن هذه القواعد تطبق أيضاً كلما كان هناك سجلات مرتبطة بالأمور الصحية يتم الاحتفاظ بها من قبل إدارة الموارد البشرية. ويستطيع أي مدير مهتم أن يحصل على المزيد من المعلومات المتعلقة بقانون HIPAA من هذين المصدرين الهامين:

١. U.S. Department of Health and Human Services (وزارة الصحة والخدمات البشرية الأمريكية): نسخ من قواعد قانون HIPAA ووسائل دعم مرجعية أخرى يمكن الحصول عليها عن طريق زيارة الموقع:

www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

٢. HIPAA Advisories (الإرشادات الخاصة بقانون HIPAA): وهو موقع تشرف عليه نظم فونيكس Phoenix الصحية كموقع خدمات عام، ويعتبر واحداً من المصادر الجيدة للحصول على معلومات عن قانون HIPAA والموجود في العنوان: <http://www.phoenixhealth.com>

يعد الامتثال لقواعد قانون HIPAA مطلباً قانونياً في الولايات المتحدة الأمريكية. ولأن مدققي الحكومة لا يقومون بزيارة المستشفيات أو مرافق الرعاية الصحية الكبيرة ومن المؤكد أيضاً أنهم لا يقومون حتى بزيارة إدارات الموارد البشرية الخاصة بالمؤسسات التجارية، فالشخص الذي يشعر أن هناك انتهاكاً أو اختراقاً لهذا القانون، يستطيع أن يتقدم بشكوى مباشرة إلى وزارة العدل الأمريكية (Department of Justice (DOJ)). وقد يحدث هذا بالتأكيد عندما تصبح بعض المعلومات الرئيسية الموجودة في سجلات الموظف الخاصة بالتعويضات المطلوبة من شركات التأمين مكشوفة ومعروفة للعموم بسبب اختراقات أمن وسرية تلك السجلات. فلدى وزارة العدل الأمريكية DOJ نهج الامتثال الطوعي للشكاوى. لذا ينبغي على كبار المديرين المهتمين أن يكونوا على دراية ومعرفة ولو على أقل تقدير بالمستوى الرفيع أو الخطوط العريضة لقواعد قانون HIPAA وبقضايا حوكمة تقنية المعلومات المرتبطة بها. فهم أحد الأسباب القوية الأخرى لجعل المؤسسة تقوم بتطبيق ضوابط قوية تتعلق بالأمن والخصوصية في أي مجال من شأنه أن يؤثر في السجلات الطبية أو الصحية الخاصة بالموظفين.

ملاحظات:

1. Privacy Rights Clearinghouse (PRC), https://www.google.com/#hl=en&client=psyab&q=privacy+rights+clearinghouse&oq=Privacy+Rights+Clearinghouse+&gs_l=serp.1.3.0l3j0i30.0.0.1.9354.0.0.0.0.
2. "The State of PCI Compliance," Forrester Consulting, September 2007, www.rsa.com/solutions/PCI/ar/RSA_AR_State_of_PCI_Compliance.pdf.
3. العديد من المحتويات الخاصة بمشاكل TJX's يمكن العثور عليها، مثل "T.J. Maxx Data Theft Worse Than First Reported," MSNBC.com, March 29, 2007, www.msnbc.msn.com/id/17853440/ns/technology_and_science-security/t/tj-maxx-data-theft-worse-firstreported/#.Tp2
4. Robert Moeller, IT Audit, Control, and Security (Hoboken, NJ: John Wiley & Sons, 2010).

الفصل الثاني عشر

بيان خدمات تقنية المعلومات: تحقيق قيمة أكبر من عمليات تشغيل تقنية المعلومات

كما تحدثنا في الفصول السابقة، كان المستخدمون في الأيام الأولى لنظم تقنية المعلومات يلجؤون إلى مديري قسم تقنية المعلومات أو الموظفين المسؤولين عن النظم لديهم ومطالبتهم بأن يقوموا بإجراء تعديلات أو ترقيات للنظم القائمة حالياً أو أن يقوموا بإطلاق نظم جديدة. وقد كانت معظم تلك المطالب لا تتعدى كونها تقارير ورقية جديدة أو تقارير بصيغ وأشكال مختلفة. وقد اشتكى هؤلاء المستخدمون في كثير من الأحيان من سوء خدمات تقنية المعلومات إما بسبب تأخير تسليم مشاريع النظم التي قاموا بطلبها أو لأن تلك النظم المنجزة لم تكن على مستوى توقعاتهم أو لوجود العديد من المشاكل الأخرى. وكان ذلك قبل ظهور الإنترنت، أي في الأيام التي كانت فيها نظم وخدمات تقنية المعلومات محدودة جداً. وقد جرت العادة بأن يقوم هؤلاء المستخدمون بتلخيص جميع احتياجاتهم واستكمال نموذج من نماذج الطلبات الرسمية الخاصة بخدمات تقنية المعلومات التي يرغبون فيها. ثم يقوم قسم تقنية المعلومات بمراجعة الطلبات المقدمة والتي كانت في الغالب يتم التصديق عليها ووضع جدول زمني لإتمامها في أقرب وقت ممكن - أحياناً يكون الوقت المحدد للبدء في تنفيذ الطلب مناسباً وقريباً من وقت تقديم الطلب، ولكن في كثير من الأحيان يكون غير مناسب ومتأخراً كثيراً عن وقت تقديم الطلبات.

أما اليوم فإن خدمات تقنية المعلومات تعد أكثر تعقيداً من كونها مجرد تقارير مالية وتشغيلية والتي كان يتم تقديمها بصورة منتظمة في السنوات الماضية. في كثير من الأحيان نرى أن مستخدمي النظم هذه الأيام بحاجة إلى إجراء تحاليل من نوع خاص تعتمد على مخرجات أنظمة أخرى قائمة بالفعل. وقد يكون لدى مستخدمي النظم بعض الاحتياجات المتعلقة بتوقيت إجرائي استثنائي تفرضه متطلبات رفع تقارير قانونية دولية، أو قد يكون لديهم اهتمام بإحدى التقنيات الجديدة التي شاهدوها في إحدى العروض التجارية

ويرغبون في مشاهدة مثلها في المؤسسة التابعين لها. ويكون هناك غالباً العديد من النظم والأدوات المتاحة لدى إدارات تقنية المعلومات، إلا أن أعضاء إدارات مجتمع المستخدمين لا يكونون غالباً على علم بخدمات تقنية المعلومات المتاحة من خلال إدارة تقنية المعلومات في المؤسسة التابعين لها. وعلى غرار قائمة الطعام التي تقدم إلينا عند زيارة أحد المطاعم، فإن قسم تقنية المعلومات يستطيع أن يساعد مجتمع المستخدمين لديه عن طريق تقديم قائمة أو بيان بالخدمات التقنية المتاحة لديهم. ويستفيد مستخدمو موارد تقنية المعلومات غالباً من قراءة البيانات الخاصة بخدمات تقنية المعلومات عندما يقومون بطلب تلك الخدمات أو جدولتها.

إن بيان خدمات تقنية المعلومات IT service catalog عبارة عن قائمة بالخدمات التي ينبغي على قسم تقنية المعلومات في المؤسسة أن يقدمها للموظفين والعملاء وغيرهم من أصحاب المصالح. وتحتوي عادة كل خدمة من خدمات تقنية المعلومات التي يتم وصفها في بيان كهذا على ما يلي:

- **وصف الخدمة:** وهي قائمة بتطبيقات أو عمليات تقنية المعلومات الموجودة في الخدمة والتي قد يحتاج إليها المستخدم في إدارته. ويجب أن تتناسب هذه التطبيقات مع مجمل العمليات التشغيلية للأعمال ومتطلبات النظم الأخرى الخاصة بها.
- **الأطر الزمنية أو اتفاقيات مستوى الخدمة (SLAs) اللازمة لاستيفاء الخدمة:** تعد اتفاقيات مستوى الخدمة من المعاملات الثنائية (تحتوي على طرفين) التي تأخذ شكل اتفاق داخلي أو عقود غير رسمية بين إدارة تقنية المعلومات والمستخدمين. وتعتبر هذه الاتفاقيات من الأدوات الهامة جداً في حوكمة تقنية المعلومات التي سيتم الحديث عنها بمزيد من التفصيل في الفصل السابع عشر من هذا الكتاب. الفكرة هي أنه يجب أن يُذكر في بيان خدمات تقنية المعلومات الوقت الذي سيتم فيه تسليم الخدمة المشار إليها ومتطلبات إدارة المستخدم للوفاء بعروض الخدمة هذه.
- **من الذي يحق له طلب أو عرض الخدمة:** يجب أن يحدد البيان مثلاً أن هناك مجموعات خاصة من التقارير التحليلية ستكون متاحة فقط لمستويات وظيفية محددة في الإدارات المالية. وبالمثل، قد تقوم بعض الخدمات المعروضة في البيان بالنص على أن المستخدمين

الذين يطلبون تلك الخدمات يجب أن يتحملوا بشكل رسمي مسؤولية حل بعض الأخطاء أو القيام ببعض المراجعات لمخرجات نظم محددة.

• **تكاليف الخدمات التقنية:** إن فكرة أن يتم تقديم خدمات تقنية المعلومات كمورد "مجانية" داخل المؤسسة قد انتهت منذ زمن بعيد. وسيقوم الفصل السابع عشر من هذا الكتاب بتقديم بعض الدعم الإضافي لحوكمة تقنية المعلومات لإدارة وفهم التكاليف والتسعير. ومع ذلك يجب أن يحدد بيان خدمات تقنية المعلومات بعض الإرشادات التي تتعلق بتكاليف الخدمات المعروضة في البيان.

• **كيفية الوفاء بالخدمة المذكورة في البيان:** ينبغي أن يكون هناك بعض المعلومات بشأن توقيت تسليم الخدمة ومستويات الموافقة المطلوبة وغيرها من المعلومات الضرورية المتعلقة بالخدمة المطلوبة من البيان.

على الرغم من أن بيان الخدمات يُعتبر واحداً من الأدوات الهامة بالنسبة لإدارات تقنية المعلومات، فإنه أيضاً مهم وذو قيمة بالنسبة للعديد من الإدارات الأخرى غير العاملة في تقنية المعلومات وحتى بالنسبة للعروض المتعلقة بإدارة الموارد البشرية. فعلى سبيل المثال، يمكن استخدام تطبيق عرض خدمة لتسجيل استحقاقات الموارد البشرية للموظف أو تغييرها أو تعديل الاشتراكات أو المصروفات من حسابات الإقراض أو حسابات الادخار للموظف، أو الإقرار بالموافقة على مدونة قواعد السلوك الخاصة بالموظف.

يمكن لإدارات تقنية المعلومات في المؤسسة أن تقوم بنشر عروض الخدمة لديها بشكل فعال من خلال موقع المؤسسة على شبكة الإنترنت والمتاح فقط لأصحاب المصلحة المصرح لهم. يستطيع المستخدم بعد ذلك القيام بزيارة الموقع للبحث عن خدمة محددة مثل طلب جهاز حاسب آلي محمول جديد، أو طلب تعديل الاستحقاقات، أو القيام بإضافة موظف جديد في أحد الأقسام في المؤسسة. يقوم هذا الموقع الخاص ببيان الخدمات بإعادة تجميع الخدمات المعروضة حسب الفئات أو الأصناف التي تنتمي لها ويسمح باستخدامها في عمليات البحث (خاصة عندما يكون هناك مئات بل آلاف الخدمات المتاحة). حيث يقوم المستخدم باختيار الخدمة التي يريدّها ومشاهدة الوصف والتفاصيل المتعلقة بها. كما يقوم المستخدم بإدخال أي معلومات تتعلق بالخدمات، كمعلومات الاتصال أو أسئلة

متعلقة بالخدمة، ثم يقوم بتقديم طلب للحصول على الخدمة المطلوبة. يحتاج طلب الخدمة إلى الموافقة أو التصديق عليه، ثم يمر من خلال عملية التوجيه وعملية إدارة مستوى الخدمة وغيرها من العمليات اللازمة لاستيفاء الطلب. يستطيع المستخدم العودة إلى الموقع لاحقاً لفحص حالة الطلب أو لاستعراض جميع المقاييس المتعلقة بمدى نجاح الإدارة في أداء الخدمات التي تقدمها.

يعد بيان خدمات تقنية المعلومات أحد الأدوات القيّمة والهامة للحوكمة بالنسبة للعديد من المؤسسات. يأخذ هذا الفصل بعين الاعتبار كيفية وضع وتطبيق بيان فعال لخدمات تقنية المعلومات، كما يأخذ بعين الاعتبار أيضاً بعض الضوابط الرئيسية اللازمة لتحسين عمليات حوكمة تقنية المعلومات ذات العلاقة. ونظراً لأن إدارة تقنية المعلومات هي التي تقوم بوضع المعايير والضوابط لتحديد الموارد التي يجب إدراجها على أنها خدمات لتقنية المعلومات في بيان خدمات تقنية المعلومات الخاص بها، ولأن هذا البيان يعمل على تحديد الخيارات المتاحة للمجتمع المستخدم لتقنية المعلومات المؤسسية، فإن بيان الخدمات المنظم والمحكم جيداً يمكن اعتباره أحد العناصر الهامة في الحوكمة الفعالة لتقنية المعلومات.

أهمية بيان خدمات تقنية المعلومات:

نظراً لزيادة الطلب من قبل وحدات الأعمال لخدمات جديدة في تقنية معلومات ومستويات أعلى للخدمة، وكذلك الضغوط المستمرة للتكاليف، فقد قامت العديد من وحدات التشغيل الكبيرة لتقنية المعلومات المؤسسية بإجراء تحولات وتغييرات جذرية خاصة في السنوات الأخيرة. فقد أدرك الرئيس التنفيذي للمعلومات (CIO) وغيره من المسؤولين التنفيذيين لتقنية المعلومات أن هناك حاجة إلى تحقيق مواءمة أو توافق أفضل بين الخدمات التي يقدمونها واحتياجات العمل، وإلى تحسين رضا العميل الداخلي، ونشر عمليات معيارية لتحقيق كفاءة تشغيلية أكبر. إن هذا الإصرار على تحسين جودة الخدمات - وإظهار قيمة الأعمال - قد دفع العديد من إدارات تقنية المعلومات إلى تطبيق عمليات محسنة للخدمات، مثل عمليات آيتل والتي تمت مناقشتها في الفصل السادس من هذا الكتاب، بالإضافة إلى بعض المنهجيات الأخرى لعملية تقنية المعلومات. ويعد بيان خدمات

تقنية المعلومات أحد المكونات الرئيسية والذي تدعو الحاجة إليه لتحسين خدمة عملاء تقنية المعلومات.

ويعتمد إطار العمل آيتل على المفاهيم الخاصة بالعناية بخدمات تقنية المعلومات وعملائها. حيث يكون بيان خدمات تقنية المعلومات في قلب تلك المفاهيم الأساسية. وقد انتجت العديد من إدارات تقنية المعلومات بيان الخدمة كجزء من نشر إدارة مستوى الخدمة طبقاً للإطار آيتل. على أية حال، حتى لو كانت المؤسسة إلى الآن لم تتبن جميع مفاهيم آيتل، فقد يكون بيان الخدمات المؤسسية بمثابة نقطة محورية لتحقيق التفاعل بين تقنية المعلومات والأعمال، كما يمكن أن يمنح كل منهما فرصة تحسين الخدمات المقدمة لعملاء تقنية المعلومات. إن بيان خدمة تقنية المعلومات يعد أحد الأدوات الهامة لحوكمة تقنية المعلومات، كما أنه ضروري أيضاً لتوفير الأساس من أجل تحديد الخدمات والتواصل مع الأعمال.

ولكي يكون بيان خدمات تقنية المعلومات فعالاً، فإنه يجب أن يُفهم ويتم تبنيه واستخدامه من قبل الأعمال. لقد أصبحت بيانات خدمات تقنية المعلومات هي المفهوم الجديد "الساخن" منذ بضع سنوات، إلا أننا نجد غالباً أن إدارات تقنية المعلومات تستهلك ساعات طويلة لتقوم بإنشاء وثيقة بيان الخدمات الخاصة بها، مستخدمةً في ذلك صيغاً ثابتة وجامدة ولا يقوم بقراءتها أو استخدامها إلا عدد قليل من العملاء. لذا نجد أن العديد من بيانات الخدمة الثابتة هذه من النادر أن يراها أو يقرؤها المستخدمون أو صناع القرار - وتصبح غالباً في نهاية المطاف عديمة التأثير.

ولكي يتم بناء بيان فعال لخدمات تقنية المعلومات، فإنه يتعين على مديري تقنية المعلومات بالإضافة إلى مديري وحدات الأعمال في المؤسسة أن يقوموا بتحديد الخدمات التي سيتم إطلاقها لمستخدميهم النهائيين من خلال بيان الخدمة الخاصة بهم. وقد جرت العادة أن يقوم مديرو وحدات الأعمال ومحللو تقنية المعلومات بتحديد أنواع الأسئلة التي يمكن أن تُطرح من قبل مستخدمي بيان الخدمات الخاص بهم، وأن يقوموا أيضاً بتحديد الموافقات اللازمة لطلب الخدمات، وأن يذكروا أيضاً النظم والعمليات الأخرى المطلوبة لاستيفاء الطلب. فبمجرد أن يتم تحديد الخدمة وتنظيم عملية استيفائها، فإنه ينبغي

على إدارة تقنية المعلومات بناء جميع الوظائف الضرورية داخل تعريف الخدمة ومن ثم نشرها في بيان الخدمة.

إن مصطلح خدمة العملاء ليس جديداً بالنسبة للعمليات التشغيلية لتقنية المعلومات. فضلاً عن أنه في الأيام الأولى لنظم التقنية وعملياتها التشغيلية، كان قسم تقنية المعلومات في أغلب الأحيان هو الذي يقرر ما الذي يجب "تطبيقه" ومتى سيتم تطبيقه. إن التكاليف الباهظة للخدمات والنظم السيئة وعدم رضا المستخدمين عنها والتي لا تلبي احتياجاتهم، قد أدت إلى إعادة التفكير بشكل كبير من جانب إدارة تقنية المعلومات فيما يخص الخدمات التي تقدمها لمستخدميها. وقد أسهم نمو نظم الحاسبات الشخصية والإنترنت في تغيير تلك المفاهيم عبر السنين. أما اليوم فإن العديد من إدارات تقنية المعلومات وكذلك إدارة المؤسسة بدؤوا يدركوا أنهم في الأساس ما هم إلا وحدة لخدمة العملاء، فهم يعملون على تقديم الدعم اللازم للنظم وغيرها من موارد تقنية المعلومات لجميع إدارات المؤسسة التابعين لها. لقد أصبح بيان الخدمة أحد السمات الرئيسية للمساعدة في بناء الخدمات الخاصة بعملاء تقنية المعلومات ودعمها. على كل حال، ولكي نضمن وجود مبادرة ناجحة لخدمات تقنية المعلومات تركز على العملاء، فإنه يجب على إدارات تقنية المعلومات اتباع التوجيهات الثلاثة التالية لبناء وتطوير بيان لخدمات تقنية المعلومات:

١- الإقرار بأن مستخدم التقنية هو الملك: بداية وقبل كل شيء يجب أن يتم إنشاء بيان بخدمات تقنية المعلومات مع التركيز القوي على حاجات العملاء الداخليين. إن الخطأ الأكثر شيوعاً الذي تقع فيه معظم إدارات تقنية المعلومات هو محاولة التركيز أكثر على شرح الخدمات التي يقدمونها من منظور تقنية المعلومات. فعادة لا يكون لدى عملاء تقنية المعلومات الرغبة في استعراض أوصاف تفصيلية للخدمة من خلال "عبارات تقنية". بل يرغبون بمشاهدة شروحات للخدمات المقدمة بعبارات يستطيعون فهمها ومكتوبة بمصطلحات غير تقنية، ومعالجة الشواغل أو الاحتياجات العاجلة.

يتم تحديد البيانات الناجحة لخدمات تقنية المعلومات اعتماداً على العميل وتأثيره داخل المؤسسة بدلاً من البنية التحتية من حيث تأثيرها في الخارج. وكناحية إرشادية، فإن البيانات الناجحة لخدمات تقنية المعلومات يجب بناؤها بطريقة مشابهة للبيانات

الحقيقية الموجودة عبر الإنترنت والتي تستخدم يومياً من قبل العملاء. مثل بيانات الخدمة الخاصة بـ أمازون دوت كوم Amazon.com، ودل Dell، وإي باي eBay.

يجب أن يشبه بيان خدمات تقنية المعلومات أحد هذه البيانات الخاصة بالعملاء والمنشورة على شبكة الإنترنت. وذلك من خلال استخدام توصيفات سهلة الفهم وواجهة استخدام سلسلة لاستعراض جميع عروض الخدمات المتاحة في البيان. يعمل البيان الفعال لخدمات تقنية المعلومات أيضاً على تقسيم العملاء الذين يحق لهم الوصول إلى البيان— سواء كانوا مستخدمين أم مسئولين تنفيذيين لوحدات الأعمال— ويقوم بعرض محتوى مختلف بناء على الإدارة، والأدوار، والاحتياجات، والمواقع، والصلاحيات. إن هذا النهج المعتمد على العميل في وضع البيان يساعد على ضمان تبني بيان خدمات تقنية المعلومات من قبل المستخدمين النهائيين وتوفير الأساس لنقاش متوازن لمستوى الأعمال فيما يتعلق بجودة الخدمة ومواءمات التكلفة مع صناع القرار في المؤسسة.

٢- جعل بيان خدمات تقنية المعلومات قابل للتنفيذ: من المهم ألا يكون بيان خدمات تقنية المعلومات أكثر من مجرد مستودع ثابت للمعلومات. فباستخدام المثال الذي طرحناه عن بيانات خدمات العملاء المنشورة على شبكة الإنترنت، حيث يقوم العملاء باستعراض البيان المنشور عبر الإنترنت على موقع أمازون. كوم Amazon.com أو دل. كوم Dell.com، وعند مشاهدتهم لشيء ما يريدونه، فيمكنهم طلبه. بالمثل، يجب أن يرتبط بيان خدمات تقنية المعلومات المقدمة للمستخدمين النهائيين مع عمليات طلب الخدمة - وذلك من خلال واجهة عربية التسوق القائمة على الإنترنت والتي تمكن المستخدمين النهائيين من طلب الخدمات وتتبع حالة الطلب عبر الإنترنت. على نحو مماثل، يجب أن يكون لدى مسئولي وحدات الأعمال التنفيذيين عرض فريد لبيان خدمات تقنية المعلومات الخاصة بالمؤسسة التابعين لها، وذلك لمنحهم مستوى أكبر من الشفافية على بنود ميزانية تقنية الأعمال ودوافع الاستهلاك ومستويات الخدمة وتأثير الأعمال على كل خدمة من الخدمات التي توفرها تقنية المعلومات.

تعد خدمات تقنية المعلومات أمراً هاماً بالنسبة للموظفين، وذلك عندما يرغبون في تحديث نظم الحاسبات المحمولة الخاصة بهم أو زيادة حجم صندوق البريد الإلكتروني

الخاص بهم. كما أنها تعد مسألة هامة بالنسبة لمُسئولي الأعمال التنفيذيين عندما يقومون بمراجعة الميزانيات أو عند استلام فواتير تقنية المعلومات الخاصة بهم. هذه هي الأوقات التي يجب أن يكون فيها بيان خدمات تقنية المعلومات متاحاً وقابلًا للتنفيذ.

ولضمان نجاح هذا الأمر، يجب أن يصبح بيان الخدمات نقطة الوصول الوحيدة التي سيلجأ إليها المستهلكون في جميع احتياجاتهم المتعلقة بتقديم خدمات تقنية المعلومات الخاصة بهم، كما يجب أن يكون هذا البيان متاحاً وبسهولة تامة وفي أي وقت يحتاج فيه العملاء إلى التعرف على الأمور التي تنفذها تقنية المعلومات وكيف تقوم التقنية بتنفيذها. كل ذلك يعني أنه يجب على قسم تقنية المعلومات أن ينظر لخدمات تقنية المعلومات كما لو كانت سلعة أو منتجات. إن كبار المديرين الذين كانوا على علاقة بإدارة تقنية المعلومات في الماضي كانوا يقومون وبشكل رسمي بملء نوع من أنواع الوثائق الخاصة بـ "طلب خدمات تقنية المعلومات" وذلك عند الحاجة إلى تقرير جديد أو أحد العمليات الجديدة لتقنية المعلومات. وكانت هذه الطلبات في ذلك الوقت يتم تحويلها إلى نوع ما من أنواع اللجان الإدارية التي كانت تقوم في البداية بمراجعة الطلبات المقدمة والموافقة عليها ومن ثم تحديد أولويات التنفيذ. إن العديد من عمليات تقنية المعلومات اليوم لا تحتاج إلى نظم مخصصة وأعمال برمجية كالتي كانت موجودة في الماضي، بل يمكن تلبية احتياجات المستخدمين من خلال العديد من نظم وعمليات تقنية المعلومات الموجودة اليوم.

٣- تمكين بيان خدمات تقنية المعلومات ليصبح نظام سجلات: ينبغي أن يقوم بيان خدمات تقنية المعلومات القابل للتنفيذ بوظيفة "نظام للسجلات" الذي يجعل من الممكن إدارة وحدة خدمات تقنية المعلومات كما يدار مشروع داخل مؤسسة. فبإمكان هذا البيان الخاص بخدمات تقنية المعلومات أن يوفر الوسائل والآليات الضرورية لإدارة طلبات العملاء، وأن يناظر العمليات الخاصة بتحقيق الخدمة مقابل كل خدمة من الخدمات المقدمة، وأن يضمن الامتثال لمستوى الخدمة والدفع بالكفاءات الخاصة بالعملية وتتبع التكاليف.

لا يمكن لأي عمل من الأعمال الموجهة نحو الخدمة أن يتم بشكل فعال بدون توفير هذه البيانات المالية والتشغيلية بسهولة ويسر. فمن خلال تزويد العملاء الداخليين بنقطة

مركزية لطلب الخدمات، تستطيع تقنية المعلومات الاستفادة من هذه البيانات للتحكم في الاستهلاك بدرجة أكثر فاعلية. فمن خلال الخدمات القياسية والموثقة على نحو جيد، يمكن لفرق تقنية المعلومات أن تفرض عمليات قابلة للتكرار وقابلة للقياس لتقديم الخدمات، الأمر الذي يؤدي في نهاية المطاف إلى جودة يمكن التنبؤ بها وموثوقة بالنسبة لمستوى الخدمات المقدمة. وهذا يسمح لمسئولي تقنية المعلومات التنفيذيين من الحصول على المعلومات الضرورية لاستخدامها في المناقشات المتعلقة بالأعمال والقائمة على الحقائق مع نظرائهم فيما يخص الميزانيات والتسعير.

يمكن أن يكون بيان خدمات تقنية المعلومات حجر الزاوية للنجاح في العديد من مبادرات تقنية المعلومات التي تركز على العملاء. فمن خلال تحديد ونشر المحفظة المعيارية الموحدة الخاصة بعروض الخدمات الخاصة بالأعمال، تستطيع إدارة تقنية المعلومات تسويق القيمة الخاصة بها بصورة أكثر فاعلية وتأسيس إطار عمل للتواصل مع الأعمال الأخرى. ومن خلال جعل بيان الخدمات تشغيلياً وإجرائياً، تستطيع عمليات تشغيل تقنية المعلومات أن تساعد في توحيد عمليات استيفاء الخدمة، وإدارة الاستهلاك، ودفع عملية التحسين المستمر.

يمكن أيضاً وقف الخدمات التي لا يتكرر الطلب عليها باستمرار. وكذلك ينبغي تحسين العمليات الخاصة بتقديم الخدمات كبيرة الحجم، كما يمكن أن توفر مؤشرات الأداء الرئيسية رؤية أكبر لضبط التكاليف، وضمان الجودة الأفضل للخدمات المقدمة، وتقديم الدعم للنقاشات الخاصة بوضع الميزانية مع صانعي القرار.

من خلال بيان خدمات معمول به يركز على العميل وقابل للتنفيذ، يمكن لقسم تقنية المعلومات أن يعمل بصفة مزود موجه نحو الخدمات حيث يقوم بتلبية احتياجات عملاء الأعمال لديه بشكل فعال. من ناحية أخرى، لا بد أن ندرك أن بيان خدمات تقنية المعلومات لا يجب أن يعرض أنواع الأشياء الموجودة في بيان سيرز ريباك Sears Roebuck catalog ذي الطراز القديم الذي كان موجوداً في الماضي — والذي كان يحوي العديد والمدهش من المدخلات. لذا يجب أن يركز بيان خدمات تقنية المعلومات على العروض الهامة لتقنية المعلومات في المؤسسة.

دور بيان الخدمة في تنظيم أعمال مزود خدمات تقنية المعلومات:

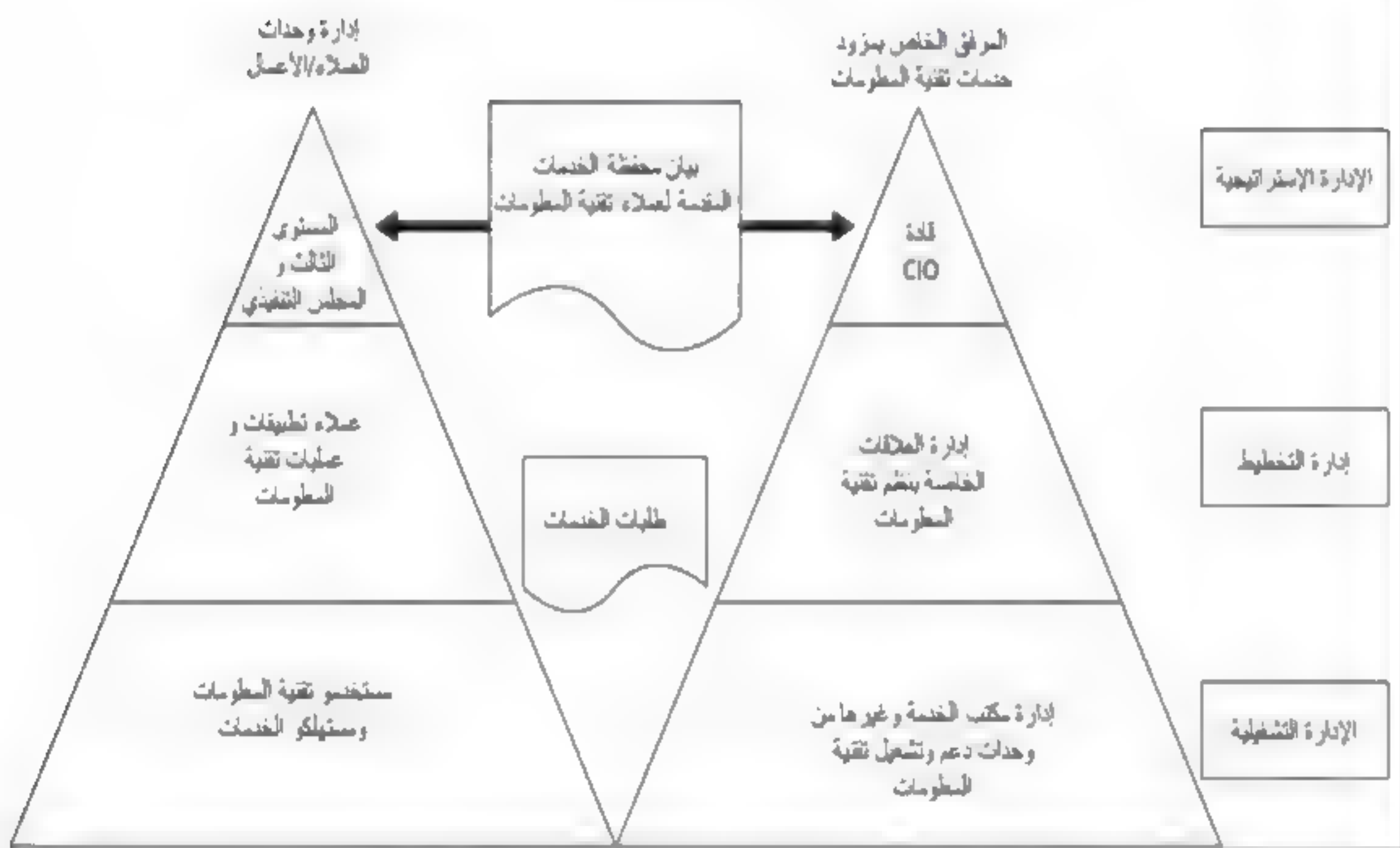
يجب أن يقدم بيان خدمات تقنية المعلومات الدعم إلى وحدات الأعمال التي ستستخدم هذا البيان بالإضافة إلى أقسام تقنية المعلومات التي ستوفر خدمات تقنية المعلومات على المستوى الإستراتيجي، والتخطيطي، وكذلك على مستوى الإدارة التشغيلية، بمعنى أن هذا البيان يجب أن يُبني أولاً على مستوى رفيع جداً بحيث يمكن لكل من الإدارة العليا وإدارة تقنية المعلومات على مستوى المدير التنفيذي للمعلومات أن يتخذوا في البداية قراراً حول أنواع العروض التي سيشملها البيان. فعلى سبيل المثال، قد تحتاج إحدى مؤسسات التجارة المالية إلى العديد من أدوات الوصول التي تساعد في إتمام أعمالها التجارية. فأي مستثمر يبحث عن برامج خاصة باختيار سوق الأسهم، على سبيل المثال، يدرك أن هناك العديد والعديد من أدوات اختيار وتحليل الأسهم. على أية حال، يمكننا القول وبكل بساطة بأنه من غير المجدي لا من الناحية العملية ولا من الناحية الاقتصادية أن يتم إدراج كل أدوات التحليل هذه في بيان المؤسسة وجعلها متاحة لأي مستوى من المستويات الخاصة بمستخدم النظام. بل ينبغي على وحدات الأعمال وقسم تقنية المعلومات أن يقوموا بفحص تلك البدائل المختلفة، وأن يضعوا فقط البدائل المقبولة أو المتعارف عليها في بيان خدمات تقنية المعلومات لديهم.

يوضح الشكل التوضيحي (١٢-١) تلك العلاقة الخاصة ببيان خدمات تقنية المعلومات بين وحدات الأعمال والإدارة الخاصة بمزود خدمات تقنية المعلومات. وليس بالضرورة أن يعبر المثلث الظاهر على يسار الشكل عن كامل المؤسسة، فهو من الممكن أن يعبر عن قسم أو وحدة أعمال أو مجموعة تشغيلية مستقلة لها مطالبها وأنظمتها الخاصة بها. فضلاً عن أن هناك وحدة معينة لنظم وعمليات تشغيل تقنية المعلومات ستقوم عادة بدعم تلك الوحدة المستقلة للأعمال. الفكرة هنا هي أنه لا بد من أن يتم وضع الإستراتيجية الشاملة لبيان خدمات تقنية المعلومات على مستوى إستراتيجي من قبل الإدارة العليا لتقنية المعلومات والإدارة العليا للتشغيل والمالية. الأمر الذي سيؤدي إلى إيجاد قيود من المستوى الأعلى تعد بمثابة الأساس لبيان خدمات تقنية المعلومات ومحفظة الخدمات الخاصة بالمؤسسة.

إن بيان الخدمة على المستوى الإستراتيجي يغطي عروضاً رفيعة المستوى لخدمات تقنية المعلومات مثل الخصائص والخيارات الرئيسية المتاحة من خلال نظام تخطيط الموارد المؤسسية (ERP) Enterprise Resource Planning والذي تم تطبيقه استناداً إلى مشروع اختيار وتطبيق البرمجيات الخاصة بأحد الباعة. إن أي نظام خاص بتخطيط الموارد المؤسسية ERP يوفر العديد من الخيارات والميزات، ويحتاج إلى مستويات عالية من التدريب والوعي لكل من المستخدمين والعاملين بهرفق تقنية المعلومات لتحقيق الاستفادة المرجوة من الميزات الخاصة بالنظام. وسنتطرق للحديث عن قضايا حوكمة نظم تخطيط الموارد المؤسسية ERP في الفصل الخامس عشر من هذا الكتاب. وسيتم تقديم نوع ERP الذي تم اختياره لأحد النظم الرفيعة المستوى في بيان الخدمة على مستوى إستراتيجي.

شكل توضيحي (١-١٢)

علاقات الأعمال الخاصة بخدمات تقنية المعلومات



ثم يأتي بعد ذلك منظور إدارة التخطيط (الإدارة التكتيكية) وهو ضروري لبناء أي بيان خدمات وتحقيق الترابط بين قسم تقنية المعلومات وإدارة عمليات التشغيل وإدارة عملاء وحدة الأعمال التابعين لها. فهي عملية مكونة من عدة خطوات وموضحة بالشكل (١٢-٢). وفي خطوة أولى، يجب على إدارة تقنية المعلومات أن تنظر بتمعن إلى موارد تقنية المعلومات الموجودة لديها والعمل على إعادة تشكيلها على أنها خدمات موجهة للمستخدمين. على سبيل المثال، قد يكون لدى إحدى المؤسسات بعض التطبيقات الرئيسية الخاصة بالمحاسبة والمالية، مثل دفتر الأستاذ العام والخاص بالإقفال في نهاية الشهر. هنا، ربما يكون من الضروري تسليط الضوء على عمليات التحليل الخاصة الأخرى ووصفها وتحديد المستخدمين المحتملين لها وإضافتها كسجلات في بيان الخدمة. هذا سيحولها من مجرد عمليات تقنية إلى خدمات خاصة بالعملاء كما هو موضح في الشكل التوضيحي (١٢-٢).

وفي خطوة تالية، يجب أن تُحوّل الخدمات التقنية الخاصة بالعملاء إلى عمليات محددة في الأعمال المؤسسية. وتفرض هذه الخطوة على فريق تقنية المعلومات وفريق الأعمال الذهاب إلى ما هو أبعد من مجرد قائمة بالتطبيقات المنفذة لديهم والتي يمكن وصفها في بيان الخدمات. الفكرة هي أنه يجب تقديم المزيد من التفاصيل التي تسمح بتمكين العمليات الخاصة بالأعمال على نحو أفضل. لذا يجب أن يحدد بيان تقنية المعلومات هذه العمليات الخاصة بالأعمال على نحو أفضل كي تسمح للمستخدمين بأن يفهموا كيفية اختيار واستخدام تلك العمليات الخاصة بالأعمال. وقد تكون الإجراءات الخاصة بالتعيينات الجديدة في إحدى وحدات المنظمة مثال على أحد أنواع العمليات التي يمكن إضافتها إلى بيان كهذا. فالوحدة التقليدية في المؤسسة لا تستقطب العديد من الأشخاص الجدد على نحو منتظم، غير أن هناك عمليات خاصة لازمة لمثل هذا الموظف الجديد، والتي تتضمن فحص المعلومات الأساسية والعروض الخاصة بخطة الاستحقاقات والتقاعد والامتنال مدونة قواعد السلوك وما هو أكثر من ذلك بكثير. فبيان تقنية المعلومات سيقود المستخدمين لتلك الخدمات الضرورية وسيوجههم إلى تحقيق الامتنال.

محتوى بيان خدمات تقنية المعلومات وسماته:

تعد بيانات خدمات تقنية المعلومات من الإصدارات الشائعة في العديد من المؤسسات اليوم. ولكن ينبغي أن تكون هذه البيانات أكثر بكثير من مجرد قوائم طويلة تحتوي على أسماء ملفات التطبيقات التي تكون أشبه بما يمكن أن نجده في قائمة أحد مجلدات أنظمة التشغيل المعتمدة على النوافذ. لذا يجب أن يتم تصميم أنواع الخدمات المقدمة لتناسب مع المنظمة وأهدافها. إن البحث في الويب عن مؤسسات أخرى قد يزودنا بالعديد من الأمثلة لما يجب أن يظهر به سجل البيانات الخاص بخدمات تقنية المعلومات، ومع أن العديد من مصادر شبكة الإنترنت تقوم بوصف منتجات البائع الذي يقوم بتسويق الحلول الخاصة به، فإنه من ناحية أخرى نجد أن بيان الخدمة النموذجي يبدأ صفحة رئيسية على الإنترنت تخص قسم تقنية المعلومات التابع للمؤسسة، حيث يلفت انتباه الأعضاء المصرح لهم بالدخول إليه من بين مجتمع المستخدمين الخاص بالمؤسسة إلى خدمات تقنية المعلومات المتاحة.

شكل توضيحي (١٢-٢)

عناصر بيان خدمات تقنية المعلومات



وعلى الرغم من أن المؤلف هنا غير محترف في تصميم مواقع الإنترنت، فإن الشكل التوضيحي (١٢-٣) يعرض مثلاً على الواجهة الرسومية الأمامية أو الصفحة الرئيسية لبيان الخدمات الخاص بالشركة العالمية لمنتجات الحاسب (Global Computer Products) التي تمت الإشارة إليها في فصول أخرى من هذا الكتاب. فبعد أن يقوم الموظف أو غيره من أصحاب المصلحة المصرح لهم بتسجيل الدخول باستخدام معرف فريد محدد وكلمة مرور خاصة به، فإنه سيمرّ هذا النوع من الصفحات الرئيسية، والتي تسرد المجالات المختلفة المتاحة لدعم النظم والتطبيقات الخاصة بها. فعلى سبيل المثال، قد يقوم المستخدم المصرح له بعد ذلك بالنقر على رابط خدمات مراقبة التطبيقات applications monitoring services. وقد تكون هذه عبارة عن أدوات خاصة لتحسين تطبيقات أخرى مخصصة للمستخدمين، حيث يشير الرقم (٥) بعد الرابط Application Services إلى عدد التطبيقات الأخرى المتاحة المتعلقة بهذه الفئة. ومع عدم مشاهدة تلك التطبيقات هنا، فإن النقر على الرابط سيعرض لنا قائمة بتلك التطبيقات الخمسة.

يمكن أيضاً عرض مجموعة من الخيارات الإضافية على أنها جزء من تلك العينة لصفحة بيان الخدمات مع روابط لصفحات أخرى تشمل:

- **طلبات الخدمة Service requests:** وستكون هذه عبارة عن بيان لعرض طلبات المستخدمين المتعلقة بالحصول على بعض التطبيقات الجديدة والخدمات الأخرى لتقنية المعلومات.

- **حالة تذاكر المشاكل Problem ticket status:** يقوم مستخدمو تقنية المعلومات الذين يواجهون مشاكل مع أي نوع من أنواع تطبيقات أو خدمات تقنية المعلومات بتعبئة نوع من أنواع الوثائق الخاصة بتذكير المشاكل، وقد سبق الحديث عنها على أنها جزء من آيتل في الفصل السادس من هذا الكتاب.

- **تاريخ التدريب Training history:** يجب أن تقدم الصفحة الرئيسية تقريراً عن حالة البرامج التدريبية المتاحة للمستخدمين حسب معرف المستخدم User ID.

- **روابط الاتصال بإدارة تقنية المعلومات:** من الممكن أن تكون روابط عامة لتقديم المساعدة.

ولأن أي بيان خدمات كهذا لن يتمكن من تغطية جميع طلبات المستخدمين، فلا بد أن يكون لدى المؤسسة إحدى العمليات المعمول بها والخاصة بالتذاكر حيث يستطيع المستخدم أن يقوم بكل من تقديم الطلبات الخاصة وفحص حالة أي تذاكر تم تقديمها. إضافة إلى ذلك فإنه يجب الاحتفاظ بسجلات دقيقة عن النشاطات التدريبية. ومن المهم توضيح أن هناك موظفين محددين قد تلقوا تدريبات في تطبيقات رئيسية وأنهم قد أتموا متطلبات تلك التدريبات.

ومن الممكن أيضاً تنظيم بيان الخدمات من خلال مجموعات من اللوحات الخاصة التي تحتوي على روابط للتطبيقات والخدمات المتاحة للموظف المستخدم. بحيث تكون تلك القائمة من الروابط مرنة وتعتمد على الصلاحيات الخاصة بدخول المستخدمين. فالمشرف في القطاع التسويقي مثلاً يستطيع أن يرى فقط الروابط الخاصة بالتطبيقات المصرح له أو لها بالوصول إليها. في حين أن لوحات أخرى تقدم للمستخدم معلومات عن أرقام الاتصال بالدعم الفني وأهم الأخبار المتعلقة بالنظم ومعلومات خاصة بالفيروسات وحالة الأمن. وقد تم الحديث عن قضايا الأمن الخاصة بتقنية المعلومات في الفصل العاشر من هذا الكتاب، كما يجب أن تكون هناك نظم معمول بها لإخطار جميع المستخدمين بالوضع الحالي للقضايا المتعلقة بالفيروسات والأمن.

تحتوي اللوحة الموجودة في الجانب الأيسر من هذا المثال للصفحة الرئيسية على قائمة من الخدمات التي ستكون متاحة للمستخدم اعتماداً على صلاحيات وحقوق الوصول الخاصة بهوية المستخدم أو المستخدمة. وتكون هذه القائمة في العادة نوعاً من أنواع الطلبات الخاصة بالتطبيقات التي لا تُدرج ضمن النشاطات اليومية الاعتيادية للمستخدمين ولكن قد تكون ضرورية لمتطلبات خاصة.

قد يكون بيان خدمات تقنية المعلومات بمثابة أداة هامة لتنظيم، وحتى التحكم نوعاً ما، بعمليات الوصول إلى موارد تقنية المعلومات الخاصة بالمؤسسة. لذلك يجب تشجيع كل من كبار المديرين ووحدات تقنية المعلومات التابعين لها على تطبيق واستخدام بيانات فعالة للخدمات والتي سوف تسمح لجميع أصحاب المصلحة المعنيين في المؤسسة باستخدام موارد تقنية المعلومات داخل حدود مسؤولياتهم بشكل فعال.


إدارة بيان خدمات تقنية المعلومات:

ربما يكون اهتمام بآئعي تقنية المعلومات والإعلام التقني المرتبط بتقنية المعلومات هو السبب وراء جعل بيانات خدمات تقنية المعلومات أحد الأشياء العصرية التي يمكن تطبيقها بالنسبة للعديد من المؤسسات خلال السنوات الأخيرة. من ناحية أخرى فإن بذل الوقت والموارد على تطبيق كهذا لن يعود بقيمة كبيرة على المؤسسة ما لم يتم تخطيط، وتنفيذ، وإدارة الجهود بشكل فعال في أرجاء المؤسسة كافة. فعمليات إدارة بيان الخدمات تمنح تقنية المعلومات القدرة على التحكم بالمبادرات الداخلية لتطوير وتقديم الخدمات ودعمها عند تأسيس الشراكة مع المستهلكين الذين سيحصلون على الخدمات المتفق عليها بمستويات وأسعار متوقعة. وتتضمن فوائد الإدارة الفعالة لخدمات تقنية المعلومات ما يلي:

- إيجاد ثقافة تقديم خدمة والتي أسهمت في تغيير النظرة التي ننظرها لإدارة تقنية المعلومات من مجرد قسم من أقسام الشركة إلى أن تكون مزود خدمات.
- توفير مصدر للمعلومات الموثوقة لإدارة استثمارات تقنية المعلومات على نحو أفضل.
- رفع مستوى الرضا لدى العملاء عن طريق السماح لهم باختيار المستويات الصحيحة لخدمات تقنية المعلومات التي تلبي رغباتهم.

شكل توضيحي (٣-١٢)

الصفحة الرئيسية لبيان خدمات الشركة العالمية لمنتجات الحاسب



Information Technology Division

Global Computer Products

IT Service Catalog Home Page

User-ID:

Password:

FIND a Service:

[A-Z Listing](#) | [Recently Added](#) | [Print Version](#)

- **Application Services (5)**
Application Monitoring Services, Call Center Management (Operator Services), Custom Application Development
- **Communication/Collaboration Services (23)**
ActiveSync Wireless Messaging Services (iPhone, Windows Pocket PC, Palm, smartphone), BlackBerry Wireless Messaging
- **Connectivity Services (10)**
Paging Network Support, Cable Management—Inter/Intra Building Connectivity, Consolidated Network Monitor
- **Enterprise Applications IT Support (3)**
Business Intelligence Services, Enterprise Application Services, Enterprise Directory Services
- **Hosting Services (7)**
Co-Location Services, Database Hosting Services, Google Search Engine Service, Mainframe Hosting Services
- **Infrastructure Services (13)**
Active Directory Development and Testing Services, Active Directory Management and Operations Services, Desktop
- **Professional Services (5)**
Consulting Services, General IT Security Services, IT System Security Assessment and Authorization Relationships
- **Support Services (10)**
Deskside Support Services, eDiscovery Services, Media Sanitization Service, Messaging and Infrastructure Support
- **Training Services (3)**
Custom IT Training, IT Training Facilitation (Classroom Rental), IT Training

Please contact the [Global Computer Products IT Service Desk](#) if you need any additional information about services in this catalog.

ينبغي على إدارات تقنية المعلومات أن تقوم بتعبئة مواردها، بموافقة الإدارة العليا، لبناء وصيانة بيان خدمات تقنية المعلومات الذي يحتوي على معلومات دقيقة عن كل خدمة من الخدمات الموجودة وعن تلك التي تم إعدادها لتعمل بشكل تشغيلي.

إن الجهد المبذول لتطوير بيان خدمات مثل هذا سيعود بفوائد كبيرة على الصعيدين الداخلي والخارجي. فعلى الصعيد الداخلي، ينبغي على إدارات تقنية المعلومات أن تقوم بتطوير وإطلاق خدماتها بناء على المتطلبات المستمدة من إستراتيجيات الأعمال في المؤسسة. أما على الصعيد الخارجي، فيستطيع عملاء تقنية المعلومات فهم توجهات تقنية المعلومات وطلب الخدمات ومستوى الخدمة التي تستطيع أن تقدمها لهم تقنية المعلومات.

تتضمن الخطوات الرئيسية للقيام بإنشاء بيان خدمات فعال لتقنية المعلومات وإدارة تلك العمليات بشكل فعال، ما يلي:

• **توثيق تعريف خدمة تقنية المعلومات:** يعد التوصل إلى توافق ينتهي بتوثيق تعريف خدمات تقنية المعلومات بمثابة الخطوة الأولى، وربما تكون الأكثر صعوبة في هذا المقام. فالسؤال هنا موجه لكل من إدارة تقنية المعلومات وإدارة المستخدمين "ما المقصود بخدمة تقنية المعلومات؟" إن الإجابة عن هذا السؤال ليست بالأمر السهل، ومن المحتمل أن تكون إدارة تقنية المعلومات قد بذلت الكثير من الوقت قبل الوصول إلى تعريف محدد وواضح للخدمة. إلا أن الإطار آيتل الذي تم تقديمه في الفصل السادس من هذا الكتاب يقدم تعريفاً جيداً واضحاً للخدمة وهو أن: "الخدمة هي وسيلة لتقديم قيمة للعملاء من خلال تسهيل النتائج التي يريد أن يحققها المستهلك دون تحمل التكلفة أو المخاطر".

ومن الآثار التي يمكن أن تنتج عن العمليات الفعالة لإدارة بيان الخدمات إمكانية مراقبة وفهم التغيرات التي تحدث على متطلبات وخدمات الأعمال. لذا يجب أن تتلقى إدارة تقنية المعلومات معلومات عن الأعمال على أنها مدخلات من وحدات الأعمال في المؤسسة حتى تتمكن من وضع الخطط الإستراتيجية والمالية لتقنية المعلومات. اعتماداً على المتطلبات الحالية والمستقبلية الموجودة في محفظة الخدمات الحالية لتقنية المعلومات. وهذا سيسمح لبيان الخدمات أن يصف بدقة جميع الخدمات التي سيكون هناك حاجة إلى نشرها. وقد تتضمن هذه المعلومات التفاصيل المتفق عليها بخصوص مستويات الخدمة

وعلى مسائل أخرى كالوقت المناسب للتسويق والتغيرات التي طرأت على العمليات الرئيسية للأعمال المعتمدة على خدمات تقنية المعلومات.

كما سيحتوي تعريف الخدمات أيضاً على معلومات تتعلق بوحدة الأعمال التي يمكنها أن تطلب الخدمة، وعن أصحاب الأعمال ومدير الخدمة الذي سيقوم بالتصديق على طلبات الخدمات. كما يجب أن تشتمل الوثيقة أيضاً على تفاصيل وحالات جميع الخدمات التشغيلية، وأيضاً تلك التي تم نقلها إلى الإنتاجية.

• **بناء محتويات البيان:** بمجرد أن يتم توثيق تعريف الخدمات وكل المعلومات المرتبطة بها، يمكن لتقنية المعلومات إنشاء محتوى بيان الخدمات الخاص بها. وهو عبارة عن نشاط يتضمن كيفية تنظيم عروض الخدمات وتزويد المستهلك بكل التفاصيل المتفق عليها.

وربما تنتج بعض الصعوبات غير المتوقعة أثناء بناء المحتوى جراء بعض التعريفات المعقدة للخدمات. يجب أن نتذكر دائماً أن "الخدمة" قد تتضمن أنشطة أخرى، مثل المكونات الرئيسية للبنية التقنية الرئيسية بما فيها من معدات وتطبيقات وشبكات وبيانات. ومن الممكن أن يكون ذلك مجدياً في تحديد التسلسل الهرمي للخدمات الموجودة بداخل البيان من خلال إعداد وتجميع أنواع الخدمات المسجلة، متضمناً ذلك خدمات الأعمال والدعم الفني والبنى التحتية والشبكات والتطبيقات. إن سؤال العملاء عن الخدمات التي سيقومون باستخدامها وعن الكيفية التي ستسهم بها هذه الخدمات في دعم عمليات الأعمال الخاصة بهم، يمكن اعتباره أحد الوسائل البسيطة للقيام بهذا النشاط الخاص ببناء محتوى البيان. إن تطوير وملء ما يعرف بـ قالب تعريف خدمات تقنية المعلومات والموضح في الشكل التوضيحي (١٢-٤) قد يكون هو نقطة البداية الرئيسية لهذه العملية. فملء تلك القوالب المعرفة مسبقاً لتعريف الخدمات ومن ثم توزيعها بين أصحاب المصلحة الرئيسيين لمراجعتها والموافقة عليها سيسهل كثيراً من هذه المهمة.

• **إنشاء نوافذ لخدمات الأعمال:** يعد وجود حاجة لفهم طرق عرض خدمات الأعمال جزءاً أساسياً من عملية تطوير بيان خدمات تقنية المعلومات، إذ تشتمل طرق العرض هذه على تفاصيل كثيرة تتعلق بجميع خدمات تقنية المعلومات المقدمة للعملاء، كما تحتوي أيضاً على توصيفات وتفاصيل يستطيع أن يفهمها العميل، وتحتوي كذلك على العلاقات

الموجودة بين وحدات وعمليات الأعمال المعتمدة على خدمات تقنية المعلومات. فمفهوم خدمة الأعمال هي نافذة العميل على بيان خدمات تقنية المعلومات كما أنها تسهم في تطوير عملية أكثر فاعلية لإدارة مستوى الخدمة.

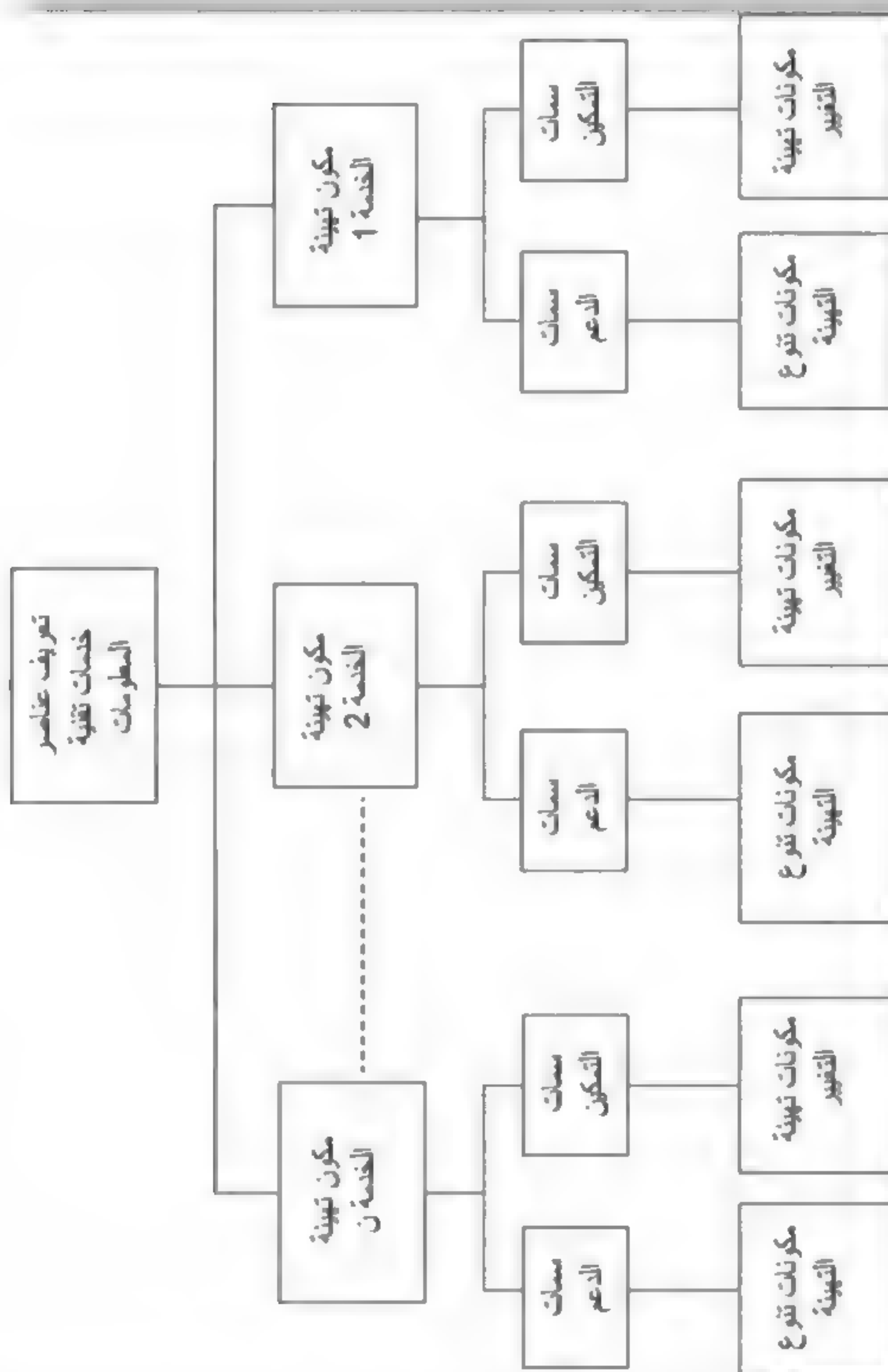
قد تساعد الحلول التقنية المستخدمة في إنتاج طرق لعرض خدمات الأعمال، الأمر الذي يسمح لتقنية المعلومات باتخاذ قرارات حاسمة حول الخدمات التي يتم طلبها وعدد المرات التي تُطلب فيها ومعرفة احتمالية دمج بعض الخيارات التي من الممكن أن تكون مرتبطة بالخدمة ومستويات الخدمة التي من الممكن أن تُطلب.

• إنشاء طرق لعرض الخدمات التقنية: نظراً لهيكل خدمات تقنية المعلومات، فإن هناك العديد من خدمات الدعم الفني تكون غير مرئية بالمرّة لمستخدمي وعملاء تقنية المعلومات، والتي يجب أن تبقى كذلك، إلا أنها أساسية وضرورية لتقديم خدمات تقنية المعلومات. يختلف بيان الخدمات التقني عن منظور خدمات الأعمال، فهو يحتوي على تفاصيل جميع خدمات تقنية المعلومات التي تم تقديمها للعميل إلى جانب علاقاتها بخدمات الدعم، والمكونات، وعناصر التهيئة اللازمة لدعم تقديم الخدمات للأعمال.

إن العديد من المؤسسات تقرر الاحتفاظ ببيان خدمات أعمال فقط أو بيان خدمات تقنية فقط. على أية حال، فإن الوضع المفضل الذي تم تبنيه من قبل المؤسسات الأكثر نضوجاً هو الاحتفاظ بكلا الجانبين بداخل بيان خدمات واحد يعتمد على الأدوار. فهو يسمح لمستخدمين مختلفين من الوصول إلى شاشة الأعمال أو شاشة الدعم التقني أو الشاشتين معاً وفقاً لصلاحياتهما.

شكل توضيحي (٤-١٢)

قالب تعريف بيان خدمات تقنية المعلومات



• **نشر الخدمات النشطة في بيان الخدمات:** خطوة أخيرة ومهمة إدارية هامة للغاية، يجب أن تقوم إدارة تقنية المعلومات بنشر بيان الخدمات الخاصة بها لعملائها. ويعد ضبط وتطوير واجهة تعتمد على الويب تسمح بالوصول إلى الخدمات المعروضة هو الحل الطبيعي في هذه الحالة. ويوضح الشكل التوضيحي (١٢-٣) مثل هذه الصفحة الرئيسية لبيان خدمات منشور على شبكة الويب.

إن إجراء الدراسات المتعلقة بإمكانية وسهولة وفحص الأداء بشكل مسبق يعد من الممارسات الجيدة في هذه الحالة. آخذين بعين الاعتبار اختلاف أنواع ومستويات الموظفين التي يمكن أن تكون موجودة بداخل هيكل المؤسسة. ومن المهم أيضاً النظر في أدوار وصلاحيات المستخدمين في وحدات الأعمال الخاصة بهم وفي السياسات الخاصة بالمنظمة. لذا يجب أن يُبنى بيان الخدمات بشكل يسمح للمستخدمين بطلب الخدمات التي يرغبون فيها بسهولة لهم وبالنيابة عن الآخرين. كما يجب أن يحتوي البيان على تسهيلات للموافقة على طلبات الخدمات المقدمة. يمكن لهذه الأمور الخاصة ببيان الخدمات أن تجعل حياة إدارة تقنية المعلومات أسهل بكثير في التمهيد لتقديم نظام جديد.

قبل نشر أي بيان لخدمات تقنية المعلومات، ينبغي على كل من قسم تقنية المعلومات والمستخدمين الأساسيين أن يقوموا بفحص جميع الأمور المتعلقة بالمنتج. وهو أشبه بالفحوصات الضرورية المتعلقة بضمان جودة أي مبادرة جديدة. إن فحص بيان الخدمات يعني ضمناً فحص الوظائف التقنية التي تعد الهدف الطبيعي من الخدمة إضافة إلى فحص أكثر مدى إمكانية استخدام الشخصي. فكل الأمرين هام لتحقيق النجاح الكلي وتبني أي بيان لخدمات تقنية المعلومات.

إن بيان خدمات تقنية المعلومات عبارة عن عملية إدارية هامة مسؤولة عن إنتاج ووصف لجميع خدمات تقنية المعلومات والاحتفاظ به. كما أن المعلومات الموجودة في بيان الخدمات المخطط له والمعد على نحو جيد ينبغي أن تعد لتعمل بشكل تشغيلي كما ينبغي أن تضمن أن المعلومات الخاصة بخدمات تقنية المعلومات المتفق عليها متاحة بشكل واسع لأولئك الذين لهم حق الوصول إلى تلك الخدمات.

تستطيع التقنية أن تلعب دوراً هاماً في تحسين عملية إدارة بيان الخدمات من خلال أتمتة الأنشطة الفعلية للعملية وبناء عروض خدمات من خلال بنية وحدة الأعمال، وأيضاً من خلال الوصول إلى المخرجات الناتجة من عمليات أخرى مرتبطة ببيان الخدمات. إن بيان الخدمات الفعال لأعمال تقنية المعلومات والمدار بشكل جيد يعد من العناصر الفعالة للحكومة الرشيدة لتقنية المعلومات.

الجزء الرابع

بناء أنظمة حوكمة تقنية معلومات فعالة ومراقبتها

٤١٢

الفصل الثالث عشر

أهمية البنية الموجهة نحو خدمات تقنية المعلومات لنظم حوكمة تقنية المعلومات

يعلم المحترفون الذين عملوا مع نظم وتطبيقات تقنية المعلومات على مر السنين أن الأساليب والتقنيات المتبعة في عالم تقنية المعلومات دائمة التغير والتطور. ففي أغلب الأحيان نرى أن المفهوم الذي كان يعتبر جديداً وساخناً منذ سنوات قليلة فقط سرعان ما يندثر ويستبدل بمفهوم آخر جديد ومختلف كلياً. ونرى في حالات أخرى أنه سرعان ما تتطور وتتحول المفاهيم التي كانت في يوم من الأيام عبارة عن مفاهيم متقدمة جداً أو حتى غريبة بعض الشيء إلى ممارسات اعتيادية ومقبولة. إن تجهيزات وإعدادات نظام الحاسبات القائم على الخادم - العميل يعد واحداً من الأمثلة على هذا النوع من الممارسات. فربما كانت تلك الإعدادات في منتصف تسعينيات القرن الماضي تعد من المفاهيم الجديدة والمختلفة، إلا أنها الآن أصبحت اللغة المعيارية الموحدة في تقنية المعلومات. نجد أيضاً أن إدارة تطبيقات تقنية المعلومات من خلال البنى الموجهة نحو الخدمات Service Oriented Architecture (SOA) تعد هي الأخرى من المفاهيم الجديدة نسبياً والتي ستصبح قريباً جزءاً من اللغة القياسية الموحدة في تقنية المعلومات. إننا نستخدم هنا الاختصار SOA مع أن هناك آخرين يستخدمون أحياناً الاختصار Software as a Service (SaaS) (البرمجيات كخدمة) للدلالة على المفهوم نفسه. فكلا الاختصارين يعني الشيء نفسه، إلا أننا نستخدم الاختصار SOA خلال هذه الفصول خلال شرحنا لهذا المفهوم.

إن البنية الموجهة نحو الخدمات SOA هي إحدى وسائل نظم تقنية المعلومات التي يتم من خلالها تجزئة الوحدات الإجرائية المنطقية الخاصة بتطبيقات الأعمال أو الوظائف الفردية وتقديمها خدمات للتطبيقات الخاصة بالمستهلكين أو المستخدمين. إن الفكرة الأساسية هنا هي أن تكون خدمات تقنية المعلومات التي يتم تقديمها فعلياً بعيدة ومستقلة كلياً عن التنفيذ الفعلي للتطبيق أو النظام. الأمر الذي يجعل مطوري نظم تقنية المعلومات قادرين على بناء وتكوين تطبيقات جديدة من خلال اختيار وتجميع المكونات

المختلفة لتقنية المعلومات. وهذا أشبه بالطريقة التي يقوم بها الطفل ببناء شكل جديد باستخدام قطع مختلفة من لعبة الليغو^(١) LEGO.

سيقوم هذا الفصل بتقديم المفاهيم الخاصة بالبنية الموجهة نحو الخدمات SOA لنظم وتطبيقات تقنية المعلومات، كما سيناقش أيضاً قضايا الرقابة الداخلية وحوكمة تقنية المعلومات الخاصة بتطوير تطبيقات تقنية المعلومات وعملياتها التشغيلية باستخدام هذه التقنية. يعد مفهوم البنية الموجهة نحو الخدمات SOA من المفاهيم التي تتطور بفاعلية وسرعة في مجال تطوير وتنفيذ التطبيقات الخاصة بتقنية المعلومات. فعندما يتحدث العاملون بإدارة تقنية المعلومات في المؤسسة عن البنية الموجهة نحو الخدمات SOA ويقومون باستخدام هذا المصطلح كما لو كان تعبيراً جديداً ومؤثراً، فإنه يجب على مديري الأعمال أن يتمتعوا بمستوى فهم عام فيما يخص هذا المفهوم، وكذلك الضوابط الداخلية والمفاهيم المحيطة بتطبيقات البنية الموجهة نحو الخدمات SOA.

تطبيقات البنية الموجهة نحو الخدمة (SOA) وتطبيقات تقنية المعلومات المدفوعة بالخدمة:

يقوم بائعو الأجهزة والبرمجيات غالباً وكذلك مطورو تطبيقات البرمجيات العالية المستوى باستخدام مصطلحات متشابهة ولكنها مختلفة قليلاً أثناء حديثهم عن مفاهيم البنية الموجهة نحو الخدمات SOA. فربما نسمع تعبيرات كالهياكل الموجهة نحو الخدمة Service-Oriented Architectures والتصميم الموجه نحو الخدمة Service-Oriented Design والتصميم الموجه نحو الهدف Object-Oriented Design أثناء الحديث عن خصائص بعض التطبيقات الجديدة لتقنية المعلومات. فهذه التعبيرات تبدو متشابهة وتشير عموماً إلى الأساليب والطرق نفسها التي يتم من خلالها بناء وتطوير تطبيقات تقنية المعلومات ونشرها في عالمنا اليوم الموجه نحو الإنترنت. وسنقوم عموماً في هذا الفصل باستخدام مصطلح البنية الموجهة نحو الخدمات Service-Oriented Architecture للإشارة إلى هذا المفهوم على الرغم من أنه قد يختلف علماء الحاسب حول بعض تفاصيل المصطلح.

إن البنية الموجهة نحو الخدمات SOA عبارة عن نمط هيكلي لتقنية المعلومات يهدف إلى تحقيق التقارن أو الارتباط الضعيف loose coupling بين وكلاء البرمجيات. وللمساعدة في توضيح التعريفات، يصف لنا هذا التقارن الضعيف loose coupling كيف يمكن للنظم المتعددة في الحاسب الآلي، حتى وإن كانت تلك النظم تستخدم تقنيات غير متوافقة، أن يرتبط بعضها ببعض لتقوم بتنفيذ المعاملات المطلوبة بغض النظر عن المعدات والبرمجيات والمكونات الوظيفية الأخرى الخاصة بتلك النظم. فعلى سبيل المثال، تعتبر الحاسبات الآلية المستخدمة في الشبكة عبارة عن نظم ضعيفة الترابط loosely coupled systems حيث يمكن لجهاز العميل أن يقوم بطلب بيانات من جهاز الخادم حتى لو كان النظامان أو الجهازان يعمل كل منهما بشكل مستقل عن الآخر.

تسمح البنية الموجهة نحو الخدمات SOA بتحقيق التشغيل البيئي أو التبادلي بين النظم ولغات البرمجة المختلفة لتقنية المعلومات. موفرةً بذلك أساس التكامل بين التطبيقات التي تعمل على منصات مختلفة من خلال الرسائل عبر وصلات شبكة الاتصالات. يتم بناء البرمجيات باتباع كل من المعايير المشتركة والمعايير الخاصة بالصناعة والتي هي عبارة عن مكونات محببة (مقسمة) ومعيارية. إن الخدمة هي وحدة من وحدات الأعمال التي تم إنجازها بواسطة مقدم الخدمات لتحقيق النتائج النهائية المرجوة لمستهلك الخدمة. إذ إن كلاً من مقدم ومستهلك الخدمة ما هو إلا أدوار يقوم بها وكلاء البرمجيات بالنيابة عن أصحابها.

على الرغم من أن هذا الوصف قد يبدو للبعض تجريدياً بشكل كبير، فإن مصطلح البنية الموجهة نحو الخدمات SOA ليس بذلك المفهوم الصعب. فأسطوانات الموسيقى الموجودة في منازلنا وكذلك مشغلات الأقراص المدمجة تعتبر مثلاً على مفاهيم البنية الموجهة نحو الخدمات SOA. فإذا كنت على سبيل المثال ترغب في تشغيل أحد الأقراص المدمجة، فإنك تقوم بوضع القرص الذي تريده في مشغل الأقراص لتقوم الوحدة الصوتية بتشغيله لك. فمشغل الأقراص في هذه الحالة يقوم بتقديم خدمة تشغيل الأقراص الموسيقية المدمجة. وعند الانتهاء من سماع القرص، يمكنك استبداله بقرص موسيقي مدمج آخر لسماعه. يمكنك أيضاً تشغيل القرص الموسيقي نفسه باستخدام مشغل أقراص محمول أو المشغل

الموجود بسيارتك الخاصة. فكلاهما يقوم بتقديم خدمة تشغيل الأقراص المدمجة نفسها. ولكن قد تختلف جودة الخدمة بسبب اختلاف الأنظمة الصوتية الموضوعة في كل منهما. وقد تؤدي نتائج خدمة تشغيل الأقراص الموسيقية إلى تغيير حالة المستهلك الذي يستمع إلى الموسيقى. فقد تتسبب في تغيير المزاج من مكتئب إلى سعيد. فنحن عملاء الخدمة Service Client ومشغل الأقراص هو مقدم الخدمة Service Provider وتقوم مكتبة الأقراص المادية الموجودة بدور الوسيط للخدمة Service Broker.

تماماً كما هو الحال بالنسبة لمشغل الأقراص الذي يقدم لنا الموسيقى المسجلة مسبقاً، فإن السبب وراء رغبتنا بوجود شخص آخر يقدم لنا الخدمات أو ينجز لنا الأعمال هو أنهم جميعاً يملكون مصادر مختلفة وخبراء مختصين. ويكون استهلاك الخدمة في العادة أقل تكلفة وأكثر فاعلية من أن نقوم بإنجاز الأعمال بأنفسنا. فمعظمنا يعلم بأننا لسنا أذكاء بما يكفي لنكون خبراء في كل شيء. والقاعدة نفسها تُطبق على بناء نظم البرمجيات.

ويقود هذا المفهوم الخاص باستخدام الخدمة الموسيقية لمشغل أقراص شخصي من مكتبة أقراص موسيقية إلى مفاهيم البنية الموجهة نحو الخدمات SOA. حيث تعتبر الخدمة هي البنية الأساسية لهذه البنية SOA، وأنها وسيلة للوصول إلى إمكانيات وقدرات أعمال قابلة للتكرار، ويتم تنظيمها لتكون واجهات برمجية بسيطة متاحة لجميع مزودي ومستهلكي الخدمة. يعرض لنا الشكل التوضيحي (١٣-١) هذا المفهوم الرئيسي الخاص بتكوين البنية الموجهة نحو الخدمات SOA، كما يعرض الشكل الآلية التي يقوم من خلالها العميل أو طالب الخدمة بطلب الخدمات من المقدم أو المجمع للخدمات من خلال وجود دليل أو بيان خاص بعروض الخدمات المتاحة لديهم. حيث سيقوم هذا البيان بسحب طلب الخدمة من أي مزود خدمة من بين العديد من مزودي الخدمات، وإعادة تلك الخدمة إلى طالب الخدمة ومن ثم إلى مزود الخدمة. إن مبدأ كل من بيانات الخدمات التي تم الحديث عنها في الفصل الثاني عشر من هذا الكتاب والبنية الموجهة نحو الخدمات SOA هو أن يتم تبني واستخدام إحدى بيانات الخدمات المتعارف عليها لتقديم الخدمات المطلوبة من تقنية المعلومات.

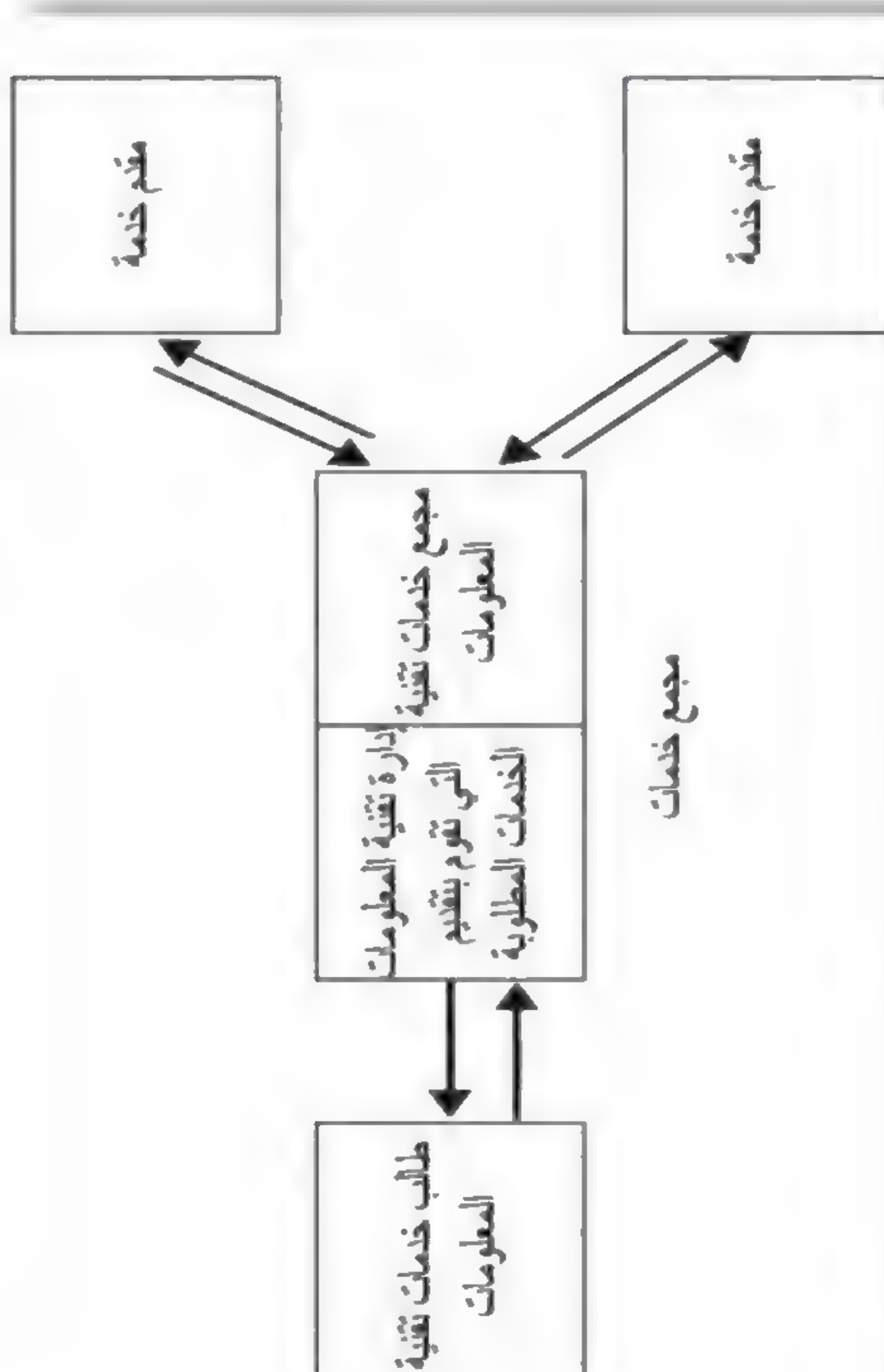
ولكي تكون البنية الموجهة نحو الخدمات SOA أكثر فاعلية، فهناك حاجة إلى أن يكون لدى جميع مستخدمي نظم وخدمات تقنية المعلومات فهم واضح لمصطلح الخدمة. والأكثر أهمية في بعض الأحيان، هو الحاجة الفعلية لإدارة تقنية المعلومات لفهم ما يعنيه مصطلح الخدمة عندما تحاول القيام بتقديم خدمات تقنية المعلومات بدلاً من قيامها بتقديم النظم والعمليات التقليدية الجديدة. فخدمة تقنية المعلومات IT Service عبارة عن وظيفة معرفة جيداً وقائمة بذاتها ولا تعتمد على سياق أو حالة الخدمات الأخرى. تعد الخدمات بمثابة وحدات البناء بالنسبة للبنية الموجهة نحو الخدمات SOA والتي يمكن اختيارها وربطها معاً لعمل خدمات أخرى أو تجميعها في تسلسل معين لإنشاء عمليات أخرى.

يتم تنظيم الخدمات في البنية الموجهة نحو الخدمات SOA بداخل ما يسمى بالسجل، وفيه يمكن جمع خدمات منفصلة لتشكيل تطبيقات مركبة منها، ومن ثم يتم تركيب بعضها مع بعض فيما يسمى مخطط البنية الموجهة نحو الخدمات SOA blueprint. وبشكل عام تتعرض إدارة تقنية المعلومات إلى متاعب متعلقة بالبنية الموجهة نحو الخدمات SOA عندما تقوم بتقييم مجمل الضوابط العامة في المؤسسة الخاصة بها ومراجعة ضوابط محددة في التطبيقات. وعلى الرغم من أننا لا نهدف هنا إلى تحويل القارئ إلى عالم في الحاسب الآلي أو مطور برمجيات، فإن هناك العديد من المفاهيم الهامة للبنية الموجهة نحو الخدمات SOA التي قد يتعرض لها كل من المختصين في تقنية المعلومات والإدارة المعنية عند مناقشة العمليات الخاصة بالبنية الموجهة نحو الخدمات SOA، وهذه المفاهيم هي:

- **تحجب (تقسيمات) مكونات البنية الموجهة نحو الخدمات (SOA Component Granularity):** وهو يصف لنا حجم المكونات التي تشكل النظام، إذ يحاول أي تطبيق بنية موجهة نحو تقديم خدمة (SOA) أن يشكل مكونات أكبر أو مكونات محبة خشنة تعرف بخدمات الأعمال. وهي التي يتم بناؤها عادة من مكونات أخرى أصغر تدعى مكونات الحبيبات الناعمة وكذلك من خدمات فنية موجودة مسبقاً. وهذا واقعي لأن المكونات ذات الحجم الكبير تجعل عملية فهم وإدارة وإعادة استخدام خدمات البنية الموجهة نحو تقديم الخدمة (SOA) أكثر سهولة بالنسبة للمؤسسة.

شكل توضيحي (١٣-١)

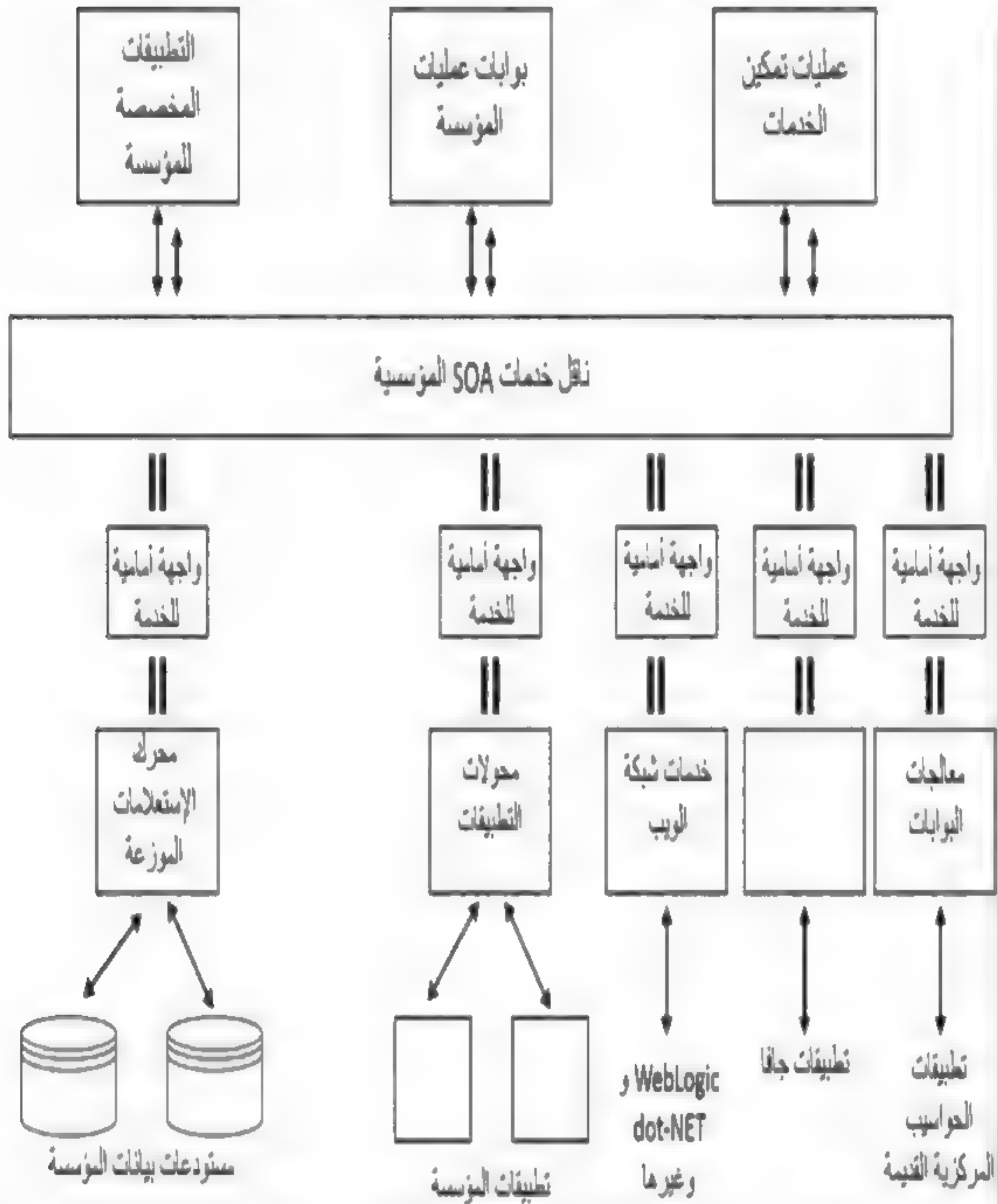
دور مجمع خدمات البنية الموجهة نحو الخدمات SOA



- **واجهة الخدمة مقابل مفاهيم التطبيق:** قم بفصل ما تفعله الخدمة عن الكيفية التي تمكنها من فعل ذلك. ويعد ذلك أمراً هاماً نظراً لتبسيطه للمبدأ الذي يشير إلى أنه يجب أن تركز رؤية مستخدم الأعمال للبنية الموجهة نحو الخدمات SOA على ما ستفعله الخدمة بدلاً من تركيزه على تفاصيل عمل التقنية غير المرئي، قياساً على نظام السيارات.
- **عقود البنية الموجهة نحو الخدمة SOA:** قم بتحديد الالتزامات بين مقدم الخدمة والمستهلك أو طالب الخدمة. وقد يتضمن ذلك احتمالات أو توقعات للخدمة مثل الإتاحة والاعتمادية ومؤشرات الأداء الأساسية KPIs والتكلفة والدعم الفني. ويعد ذلك أمراً هاماً نظراً لأنه يساعد مستخدمي الأعمال على اتخاذ قرارات أعمال منطقية وعقلانية فيما يخص اختيار الخدمات التي يمكنهم الاعتماد عليها. إن هذه المبادئ مشابهة لاتفاقيات مستوى الخدمة المطروحة في الفصل السابع عشر من هذا الكتاب.
- **مفاهيم التقارن أو الارتباط الضعيف (Loose Coupling) في البنية الموجهة نحو تقديم خدمة (SOA):** وهي الطريقة التي تستخدم لتصميم خدمات أكثر مرونة وأقل اعتمادية بعضها على بعض. ويساعد ذلك في ضم الخدمات وإعادة تجميعها معاً أو دمجها أو إعادة تركيبها. تعد البيئة الخاصة بالبنية الموجهة نحو الخدمات في ظل وجود عملية التقارن أو الارتباط الضعيف loose coupling من الأمور الهامة نظراً لأن عملية تجميع حلول الأعمال من الوحدات البرمجية السابق إنشاؤها تكون أسرع من عملية كتابة كل وظيفة عمل جديدة من البداية.
- إن عملية تبني أو اعتماد المؤسسة للبنية الموجهة نحو الخدمات SOA ليست عبارة عن عملية إجراء تطبيق واحد في المرة الواحدة ، وإنما هي بنية أو هيكلية شاملة يتم من خلالها تنظيم وربط جميع عمليات تقنية المعلومات بعضها مع بعض. فالخدمات المقدمة من خلال تطبيقات الإنترنت حيث يمكن للمستخدم من أن يقوم بسحب أي مرجع HTML فقط من خلال قيامه بالنقر المزدوج عليه لهو خير مثال على مفهوم البنية الموجهة نحو الخدمات SOA. يوضح الشكل التوضيحي (١٣-٢) التكوين الافتراضي للبنية الموجهة نحو الخدمات SOA على مستوى المؤسسة.

شكل توضيحي (٢-١٣)

التركيب الخاص بالبنية الموجهة نحو الخدمات على مستوى المؤسسة



يوجد في المستوى السفلي من الشكل مصادر بيانات المؤسسة ونظم أخرى متعددة المنصات. سيتم تعريف جميع العناصر على أنها خدمات كأحد التطبيقات الخاصة على سبيل المثال، والذي ربما تم بناؤه من خليط من مكونات الخادم أو الحاسبات المركزية القديمة أو تطبيقات الويب حيث تم تجميعها مع المكونات المطلوبة من خلال ناقل الخدمة الموائم أو التطبيق المناسب. عندما تحتاج أي من خدمات التطبيقات تلك لعنصر من عناصر البيانات (خدمة أخرى) فإنه سيتم رفع الطلب إلى ناقل الاتصالات ثم يعود إلى مصدر البيانات المناسب. سيتم بناء مثل هذا التطبيق الشامل باستخدام أدوات تطوير برامج التطبيقات المقدمة من قبل المورد (البائع) كمايكروسوفت دوت نت^(٢) Microsoft Dot Net أو أوراكل بيا ويب لوجيك^(٣) Oracle's BEA WebLogic، وسيتم تهيئته وتنسيقه من خلال عمليات محددة وواضحة.

في الغالب لن يجد المسئول التنفيذي في المؤسسة والمعني بهذا الأمر مثل هذه البيئة الكاملة للبنية الموجهة نحو الخدمات في المؤسسة التقليدية. وإنما ستقوم إدارة تقنية المعلومات المؤسسية وبدعم من إدارتها بتطبيق البيئة الخاصة بالبنية الموجهة نحو الخدمات خطوة خطوة بشكل نموذجي، متبعة في ذلك المخطط الشامل لبناء مثل هذا النموذج. فمع زيادة نمو استخدام خدمات الإنترنت التي أحاطت معظم برمجيات وبيئات تقنية المعلومات المباعة والمقدمة كمكونات برمجية مستقلة بدلاً من أن تكون تطبيقات كاملة، يستطيع كبار مديري الأعمال أن يتوقعوا مشاهدة العديد من تطبيقات البنية الموجهة نحو الخدمات المتقدمة SOA الجزئية أو حتى الكاملة.

حوكمة البنية الموجهة نحو الخدمة وقضايا الرقابة الداخلية والمخاطر:

لا تتم عملية تحول المؤسسة إلى بيئة البنية الموجهة نحو الخدمات الخاصة بتقنية المعلومات فقط من خلال قيامها بشراء حزمة من البرمجيات وبتدريب الكادر التقني على استخدامها ومن ثم افتراض توجه الكادر نحو تطبيقه والعمل به. إن البنية الموجهة نحو الخدمات SOA هي أكثر من مجرد طريقة جديدة لتنظيم نظم تقنية المعلومات الموجودة حالياً، فهي بحاجة إلى تخطيط مفصل للانتقال إلى تلك البيئة الجديدة، وكذلك إلى سياسات وإجراءات جديدة لتقنية المعلومات. وما هو أهم من ذلك، هو حاجتها إلى

تطبيق تدريجي ومنظم جداً بحيث يتم جلب عمليات تقنية المعلومات إلى بيئة البنية الموجهة نحو الخدمات SOA بطريقة مُحَكَّمة. في بعض الحالات نرى أن مزايا وفوائد العمليات التشغيلية للبيئة الموجهة نحو الخدمات SOA ستكون واضحة أمام كبار المديرين وغيرهم. على سبيل المثال، فإن أي مؤسسة قامت بتحويل قسم كبير من تطبيقاتها إلى بيئة الويب المعتمدة على جافا Java أو دوت نت Dot-Net، فإنها تستطيع غالباً وبكل سهولة تبرير وتأيد مزايا تحول أنظمتها القديمة والعمليات الأخرى إلى بيئة البنية الموجهة نحو الخدمات SOA.

ينبغي على كبار المديرين المعنيين تكوين فهم جيد وعام عن عمليات البنية الموجهة نحو الخدمات SOA، هذا بالإضافة إلى فهم بعض الخطوات الضرورية اللازمة لإدارة المؤسسة ولمهام تقنية المعلومات لديهم لكي يتم الانتقال إلى البنية الموجهة نحو الخدمات SOA. بعض تلك الخطوات تتطلب فهم الضوابط الداخلية لحوكمة تقنية المعلومات، كما تحدثنا في الفصل الرابع من هذا الكتاب. كما ينبغي أيضاً على كبار المديرين أن يكونوا مرنين مع ضوابط البنية التحتية لتقنية المعلومات الخاصة في بيئة البنية الموجهة نحو الخدمات SOA، هذا بالإضافة إلى فهمهم الجيد لضوابط إدارة المشروعات، كما سنرى في الفصل السادس عشر من هذا الكتاب. يحتاج المدير العام المهتم إلى فهم القليل من خصائص البنية الموجهة نحو الخدمات SOA وحوكمتها وقضايا الرقابة الداخلية والمخاطر المتعلقة بها. سنتحدث في هذا الفصل باختصار عن تطبيق العمليات الفعالة الخاصة بالبنية الموجهة نحو الخدمات SOA، من وجهة نظر حوكمة تقنية المعلومات. وستناقش الأقسام التالية أهمية كل من إعداد المخططات الأولية والتفصيلية لتطبيق البنية الموجهة نحو الخدمات SOA وتنظيف التطبيقات والعمليات القائمة حالياً بشكل استباقي، وتأسيس سياسات وإجراءات مناسبة للبيئة الموجهة نحو الخدمات SOA وفحص وتطبيق البنية الموجهة نحو الخدمات SOA، بطريقة فعالة.

تخطيط وبناء مخطط تطبيق البنية الموجهة نحو الخدمة وتنفيذه:

يشير الحرف الثالث للاختصار SOA إلى (البنية) Architecture، فإنشاء البنية الفعالة يعد بمثابة الخطوة الأولى الأساسية لإطلاق بيئة البنية الموجهة نحو الخدمات SOA في

المؤسسة. قد يكون المدير التنفيذي للمعلومات CIO في المؤسسة قد تعرض للمفاهيم الخاصة بهذا المصطلح أو أن تكون المؤسسة قد قامت بتنفيذ تطبيق مفرد شبيه ببيئة البنية الموجهة نحو الخدمات SOA والذي نال الكثير من التعليقات الحماسية والثناء، ولكن المؤسسة بحاجة إلى بناء خطة شاملة أو إطار عمل لإطلاق أي تطبيق أو تنفيذ أي عملية تخص البنية الموجهة نحو الخدمات SOA.

إن الفكرة الرئيسية للوصول إلى البنية الفعالة الموجهة نحو الخدمات هو تحديد الخطة الموجودة أو بناء الخدمة باستخدام الوحدات المبنية التي ستعرف SOA. وكما تحدثنا سابقاً، فإنه يجب أن تظهر خدمات SOA كما لو كانت أشبه بمجموعة من القطع الخاصة بلعبة الليغو LEGO، وهي لعبة الأطفال الشائعة حيث يمكن من خلالها تركيب تلك القطع لتكوين مجموعة مختلفة من الهياكل المعقدة ثم يتم فصل بعضها عن بعض لتركيب هيكل أو شكل آخر مختلف. على كل حال، فإن خدمات SOA أكثر من مجرد قطع خاصة بلعبة الليغو والتي يمكنها فقط أن تكون بأشكال مكعبات أو مثلثات. فخدمات SOA أوسع بكثير وقد يكون لها العديد من الأبعاد المختلفة عموماً. لذا ينبغي أن تحدد بنية SOA للمؤسسة عناصر الخدمات المختلفة الخاصة بها والمستفيدين من الخدمات، هذا بالإضافة إلى مسار تدفق النشاطات ونقاط اتخاذ القرارات بين المستفيدين المعنيين بالعملية على النحو التالي:

• **أصحاب الأعمال:** يعمل المالك أو مستخدم النظم على توفير متطلبات التطبيق اللازمة لتنفيذ أحد القدرات أو الحلول أو العمليات الجديدة الخاصة بالأعمال. كما يجب على صاحب العمل أو أعضاء فريق دعم تقنية المعلومات أن يقوموا بتطوير نماذج الأعمال business models وذلك لتسهيل فهم أي متطلبات خاصة بخدمات تطبيق تقنية المعلومات. كما يحتاج صاحب العمل أيضاً إلى تحديد المتطلبات غير الوظيفية كجودة الخدمة المتوقعة بالنسبة للقدرة أو الحل أو العملية.

• **مهندسو SOA:** لإطلاق مبادرة البنية الموجهة نحو الخدمات SOA، تحتاج المؤسسة إلى تعيين مهندس ماهر في SOA لكي يقوم بتحليل متطلبات الأعمال والخروج منها بتصاميم خدمات وأعمال. وقد يقرر مهندس SOA على سبيل المثال، أن يعيد استخدام مكونات

موجودة حالياً بدلاً من إنشاء مكونات جديدة. وعندما يقترح المهندس تنفيذ خدمة أو عملية جديدة أو التغيير في خدمة أو عملية موجودة، فإنه يجب عليه تسليم مواصفات التصميم الخاصة بمخططات الحالة والنماذج العملية وتصميم الواجهات. كما يعمل مهندس SOA على صياغة المتطلبات غير الوظيفية للمكون المراد تطبيقه بشكل رسمي متضمناً المتطلبات الخاصة بالإتاحة والأمن والأداء الخاصة به.

• **مطورو التطبيقات:** يقوم مطور التطبيقات بتنفيذ المكونات بناءً على مواصفات التصميم المقدمة من مهندس SOA، ووضع الضوابط الداخلية، ووضع خطط الفحص أو الاختبار بناءً على هذه المواصفات. وللمساعدة في تحقيق التقارب بين التقنية والمنهجية، فإنه ينبغي على مطور التطبيقات استخدام الأجزاء التي وضعها مهندس SOA من أجل التنفيذ متضمنةً الأكواد البرمجية ونموذج التحسينات.

• **مدير الجودة:** يجب على مدير الجودة في المؤسسة أن يستخدم المدخلات التي قام كل من صاحب العمل والمهندس والمطور بتقديمها لمراجعة وتدقيق مدى صحة الخدمة أو العملية التي تم تنفيذها. ثم يقوم مدير الجودة بعد ذلك باستخدام خطط الفحص أو الاختبار التي قام المطور بتسليمها ليقوم بتنفيذ اختبار الحلول المقدمة في البيئة التجريبية ويتحقق من سلامة مقاييس الجودة والآثار الجانبية والخصائص غير الوظيفية.

بمجرد أن يتم تحديد الفريق الرئيسي للعمل، فإنه ينبغي على المؤسسة تطوير مخطط بيئة SOA الذي يشير إلى حالة الهدف المطلوب، أو إلى الصورة الكاملة لما ينبغي أن يظهر به تطبيق SOA بعد اكتماله. يجب على مخطط SOA في المقام الأول أن يضع كل خدمات الأعمال التي يتعين القيام بها ومتطلبات وصف الخدمات ذات العلاقة ومقاييس الأداء ومعايير التشغيل البيئي أو التبادلي.

إن من شأن مخطط كهذا أن يقدم ملخصاً شاملاً وحتى "أوامر السير" بشأن الوضع الذي ترغب المؤسسة وإدارة تقنية المعلومات في الانتقال إليه مع SOA. بالطبع فإنه يجب على المؤسسة ألا تبدأ بتنفيذ أو حتى توافق على إستراتيجية SOA ما لم يكن هناك فهم جيد للفوائد التي سيتم تحقيقها من هذا النهج. يوضح الشكل التوضيحي (١٣-٣) بعض الفوائد الرئيسية التي يجب أن تدركها المؤسسة جراء الانتقال إلى بيئة SOA.

انتقال التطبيقات والعمليات القائمة حالياً إلى بيئة SOA:

إن انتقال العمليات والتطبيقات الموجودة سواء كانت نظاماً قديمة أو تطبيقات قائمة على الخادم أو تطبيقات أكثر حداثة كتطبيقات الهواتف المحمولة القائمة على شبكة الويب قد يشوبه بعض التحديات نفسها والتي قد يتذكرها بعض العاملين القدامى في أواخر تسعينيات القرن الماضي وهو الخوف من مشكلة العام ٢٠٠٠ (Y2K). وعلى الرغم من نسيان معظم الأخصائيين لذلك، فإن العديد من البرامج القائمة على لغة البرمجة COBOL التي تم بناؤها في تسعينيات وثمانينيات القرن الماضي أو حتى قبل ذلك الوقت، كانت بها حقول خاصة بتاريخ التقويم النظامي بالصيغة yymmdd. وقد اعتمدت العديد من القرارات البرمجية المرتبطة بتاريخ مختلفة على اتخاذ الإجراءات النظامية عن طريق ترتيب هذه التواريخ. وقد تسبب العام ٢٠٠٠ في تسجيل هذه القرارات البرمجية القائمة على التاريخ بـ ٠٠٠٠. لقد كانت المخاوف تدور حول أن العديد من النظم سوف تتوقف نظراً لتواريخ البرامج غير الصالحة والخارجة عن المدى أو التسلسل، كما أن عملية التوثيق بالنسبة للعديد من التطبيقات وقتها كانت ضعيفة. وقد بذلت الإدارات الرئيسية ومدققو تقنية المعلومات جهوداً كبيرة للاستعداد لمشكلة Y2K.

شكل توضيحي (٣-١٣)

الفوائد الرئيسية جراء استخدام بيئة SOA

فيما يلي النقاط التي يجب أخذها في الاعتبار من قبل إدارة تقنية المعلومات والإدارة العامة في تحول نظم وخدمات تقنية المعلومات الخاصة بهم إلى بيئة البنية الموجهة نحو الخدمات SOA.

- **تحسين رؤية الأعمال:** تعمل بيئة SOA عموماً على تكامل النظم الموجودة وتجميع بيانات من وجهات نظر أكثر ثباتاً ودقةً لبيانات العملاء والتي تتضمن:
 - معلومات حتى هذه اللحظة لتحسين خدمة العملاء.
 - معلومات عبر المؤسسة تستهدف (١:١) من النشاطات.
 - معلومات متناغمة ودقيقة وأكثر شمولاً تساعد على اتخاذ قرارات أفضل.
- **تحقيق مرونة الأعمال:** في حال التطبيق الكامل، بإمكان بيئة SOA إيجاد بنية تحتية لبرامج تكاملية ورشيقة لتحقيق الاستجابة السريعة لحاجات الأعمال:
 - التسليم السريع لقدرات الأعمال الجيدة.
 - يقلل الآثار الناجمة عن تغير الأعمال والتقنية.
 - حماية الاستثمارات أثناء خلق وظيفة جديدة.
- **كسب كفاءة الأعمال:** تبسيط وأتمتة وتمكين تتبع ورؤية أفضل لعمليات الأعمال في المؤسسة:
 - مشاركة وتبادل عمليات الأعمال بشكل سري داخل وخارج الجدار الناري لنظم تقنية المعلومات.
 - إنشاء جسور بين مخازن البيانات لضمان سلامة البيانات على نحو أفضل.
 - إدارة القرارات الخاصة بالأعمال بصورة استباقية من خلال مؤشرات أداء رئيسية من مصادر أخرى.
- **تحسين عمليات حوكمة تقنية المعلومات:** نظراً لقيام بيئة SOA بتصنيف وتنظيم جميع عمليات تقنية المعلومات في المؤسسة بشكل أفضل، فإنه سيتم إدارة وضبط الحوكمة والرقابة الشاملة لهذه العمليات بشكل أفضل.

وتتعرض إدارات تقنية المعلومات لبعض القضايا المشابهة عندما تخطط وتعد للتحول إلى SOA. وفي حين أن المخاوف هذه الأيام ليست في تواريخ COBOL ذات الصيغة yymdd غير الموثقة، فإن الإدارة التقليدية لتقنية المعلومات لديها طبقات من التطبيقات والبرامج والنظم الزائدة التي لا يمكن الوصول إليها في الغالب على نحو متبادل (ومشاركتها)، وكذلك العديد من التكاملات غير المتناغمة التي تحدث من نقطة إلى أخرى في تطبيقاتها. وربما تمثل هذه المشاكل التحدي الأكبر في موضوع تطبيق العمليات الفعالة لبيئة SOA. وبالنسبة لأي فريق يقوم بتطبيق بيئة SOA على مستوى المؤسسة، إذا لم يكن هذا الفريق مُلمّاً بالنظم والعمليات والهيكل التنظيمية لتقنية المعلومات القائمة حالياً فهناك احتمال قوي أن يفشل تطبيق SOA.

سياسات وإجراءات بيئة SOA:

إن المفهوم العام الشامل والرائع لبيئة SOA هو أنها تقوم باستخدام وحدات خدمية يمكن تجميعها وإعادة تجميعها أسوة بالمثل الذي أشرنا إليه سابقاً عن القطع الخاصة بلعبة الليغو. على كل حال، فإن بيئة SOA لن تعمل في المؤسسة على نحو جيد في حال قررت إحدى وحدات الأعمال فيها بأنها تريد أن تكون مختلفة بعض الشيء وأن الوحدات الخدمية الخاصة بها في الواقع لا تتناسب مع غيرها. فباستخدام مثالنا الخاص بقطع لعبة الليغو، فربما يكون هناك وحدة معينة ترغب في أن تكون القطع الخاص بها بحجم مختلف، وهي في هذه الحالة لن تتناسب مع أي من الوحدات الأخرى.

وعلى الرغم من أن هناك دائماً أسباباً وراء حاجة وحدة أو أخرى من وحدات الأعمال إلى أن تكون مختلفة (كالقضايا الأمنية العالية)، فمن الطبيعي أن تحتاج المؤسسة إلى نوع من أنواع السلطة المنوط بها وضع المعايير، وذلك لوضع السياسات وسن القوانين المتعلقة بخدمات SOA الخاصة بها. بالنسبة للعديد من المؤسسات، فإن الكيانات الحكومية التي تقوم بوضع وفرض السياسات الخاصة بـ SOA ومعايير المؤسسة تسمى عادة مراكز SOA للإبداع أو مراكز الجدارة SOA. وتتكون مراكز الجدارة تلك من ممثلين أو وكلاء من كل وحدة من وحدات الأعمال التي تتأثر بمخطط ومخطط SOA الخاصة بالمؤسسة. فتقريباً كل جزء من أجزاء مخطط SOA الخاص بالمؤسسة - متضمناً ذلك الخدمات التي سيتم بناؤها،

وكيفية تحديدها، وكيفية التشغيل البيئي لها - سيقوم بتعريف سياسات SOA الخاصة بالمؤسسة بشكل ضمني. ونظراً لاحتواء مخطط SOA الخاص بالمؤسسة على العديد من السياسات الضمنية، فمن المهم جداً أن يكون أول إجراء يتخذه مركز الجدارة الخاص بـ SOA والذي تم إنشاؤه مؤخراً، هو التصديق على هذا المخطط واعتباره هدفاً مشتركاً.

ومن المهم بالطبع بالنسبة لكل مجموعة معنية بداخل المؤسسة أن تفهم الآثار الناتجة عن مخطط البنية الموجهة نحو الخدمات (SOA) وتوافق عليها نظراً لتأثيرها في أعمالها ونشاطاتها اليومية. ولهذا السبب، فإن التصديق على مخطط SOA لا يجب أن يأخذ شكل الموافقة الروتينية دون دراسة. بل يجب على كل شخص معني التفكير ملياً ليعرف كيف ستؤثر هذه الرؤية للبنية الموجهة نحو الخدمات SOA فيهم، متضمناً ذلك النتائج الشاملة لحوكمة تقنية المعلومات.

ينبغي على المؤسسة وضع سياسات الامتثال لمتابعة وتقييم التنفيذ الإلزامي لسياسات وعمليات بيئة SOA الخاصة بها. هذا من شأنه أن يضع "قواعد الطريق" ويوفر الحكم على نشاطات بيئة SOA القائمة على المخطط المتفق عليه. إن عمليات التنفيذ الآلي مفضلة عن التنفيذ حسب المكان الذي يمكن أن تطبق فيه. على كل حال، لا يمكن أتمتة جميع السياسات، فقد يكون هناك بعض الخطوات التي تتطلب التقييم والتدخل البشري.

تغطي الحوكمة السليمة لبيئة SOA عدة نقاط إلزامية خلال الدورة الكاملة لحياة الخدمة. يصف الشكل التوضيحي (١٣-٤) أدوار ومسؤوليات الأشخاص الرئيسيين المشاركين في تطبيق بيئة SOA والذين أصبحوا جزءاً لا يتجزأ من دورة حياة تطوير النظم الخاصة بتلك البيئة. سيتم الحديث عن المفاهيم الخاصة بدورة حياة تطوير النظم (SDLC) System Development Life Cycle وأهميتها في حوكمة تقنية المعلومات في الفصل الخامس عشر من هذا الكتاب والذي يدور حول موضوع تطبيق نظم تقنية المعلومات المتكاملة. يتم تقسيم سياسات وعمليات بيئة SOA عادة إلى فئتين هما: (١) سياسات حوكمة أثناء التصميم لضمان توافق أدوات بيئة SOA مع متطلبات التصميم المنصوص عليها في مخطط بيئة SOA. (٢) سياسات حوكمة أثناء التنفيذ لضمان توافق خدمات SOA مع متطلبات التشغيل التي تم التفاوض بشأنها

بين مقدم الخدمة والمستهلك. إن هذه العمليات الخاصة بحوكمة بيئة SOA تشبه بعض الشيء اتفاقيات مستوى الخدمة SLAs التي تمت مناقشتها في الفصل السابع عشر من هذا الكتاب، حيث ستقبل العمليات التشغيلية لتقنية المعلومات بشكل رسمي بتوفير التعاملات الخاصة بمجموعة المستخدمين وفقاً لجدول زمني متفق عليه مسبقاً، كما ستقوم تقنية المعلومات بتسليم ملف التحديثات والعمليات المنجزة وفقاً للجدول الزمني نفسه المتفق عليه. فمن خلال SOA يمكن أن نقوم بعمل سلسلة من الاتفاقيات الصغيرة بين مقدمي ومستهلكي الخدمات.

شكل توضيحي (١٣-٤)

أدوار ومسؤوليات أصحاب المصلحة خلال دورة حياة بيئة SOA.

تقوم دورة حياة بيئة SOA بوصف وتنفيذ سلسلة من النشاطات ونقاط اتخاذ القرار بين أصحاب المصلحة - مستخدمين وتقنية معلومات - المعنيين بهذه العملية. ينبغي أن تشمل دورة حياة تطوير بيئة SOA الفئات التالية من المشاركين الرئيسيين:
<p>أصحاب الأعمال: يقوم أصحاب الأعمال في بيئة SOA بتوفير المتطلبات اللازمة للأعمال المزمع تنفيذها متضمناً ذلك الإمكانيات أو الحلول أو العمليات. وأفضل طريقة لصياغة هذه المتطلبات هو أن يتم وضعها في نموذج عمليات الدعم والذي يقوم بتغطية نشاط الخدمة. فاستخدام نماذج العمليات يساهم في توفير بيئة تجعل عملية فهم متطلبات تطبيق تقنية المعلومات أكثر سهولة. كما يحتاج صاحب العمل أيضاً إلى تحديد الاحتياجات غير الوظيفية (مثل جودة الخدمة) للقدرة أو الحل أو العملية.</p>
<p>المهندس المعماري لبيئة SOA: عادة ما يقوم المهندس المعماري لبيئة SOA، بصفته عضواً أساسياً في فريق تقنية المعلومات، بتحليل متطلبات الأعمال وتقسيمها إلى عناصر خاصة بتصميم عملية الخدمة. فقد يقرر المهندس إعادة استخدام أحد المكونات الموجودة بدلاً من إنشاء مكون جديد. في هذه الحالة فإنه سيقدر تحويل هذا المكون إلى عنصر في دورة حياة بيئة SOA ليتمكن من إعادة استخدام هذا المكون القائم حالياً. عندما يتم تحديد الخدمة أو العملية الجديدة أو المراد تطبيقها، فإن مهندس SOA يقوم بتسليم مواصفات التصميم في شكل مخططات الحالة ونماذج العملية وتصاميم للواجهات الأمامية. كما يعمل مهندس SOA على صياغة المتطلبات غير الوظيفية للمكون المراد تطبيقه بشكل رسمي متضمناً الإتاحة والأمن والأداء.</p>

مطور بيئة SOA: يقوم المطور بتنفيذ المكونات بناءً على مواصفات التصميم المقدمة من مهندس بيئة SOA كما يقوم أيضاً بإنشاء خطط اختبار بناءً على هذه المواصفات. وللمساعدة في تحقيق التقارب بين التقنية والمنهجية، فإنه ينبغي على المطور استخدام الأجزاء التي وضعها مهندس SOA لتطبيقها متضمناً ذلك الأكواد البرمجية وأدوات تحسين النموذج.

مدير الجودة في بيئة SOA: يستخدم مدير الجودة المدخلات التي قام كل من صاحب العمل والمهندس والمطور بتوفيرها لمراجعة وتدقيق مدى صحة الخدمة أو العملية التي تم تنفيذها. ثم يقوم مدير الجودة بعد ذلك باستخدام خطط الفحص أو الاختبار التي قام المطور بتسليمها ليقوم بتنفيذ اختبار الحلول المقدمة في البيئة التجريبية والتحقق من سلامة مقاييس الجودة والآثار الجانبية والخصائص غير الوظيفية.

مشغل بيئة SOA: يقوم المشغل باستقبال الحلول التي تم اختبارها والتأكد من صحتها ويقوم بتطبيقها داخل العمليات المعيارية لتقنية المعلومات لجعل هذا الحل متاحاً للمستخدمين والمستهلكين له. حيث يقوم هو أو هي باستخدام المواصفات التي تمت صياغتها والخاصة بالمتطلبات غير الوظيفية لتشغيل الحلول الافتراضية التي تتفق مع اتفاقيات مستوى الخدمة SLAs المطلوبة من قبل مستهلكي التطبيقات. إن الحلول الخاصة بحوكمة تشغيل SOA هي التي تقدم هذه الأنواع من القدرات من خلال فرض المتطلبات غير الوظيفية واتفاقيات مستوى الخدمة.

سياسات بيئة البنية الموجهة نحو الخدمات SOA خلال فترة التصميم:

إن العنصر الرئيسي في سياسات وعمليات بيئة SOA وقت التصميم هو ضمان أن الخدمات سيتم بناؤها وفقاً للمواصفات المحددة في الخطة الخاصة بمخطط بيئة SOA. وعلى وجه الخصوص، فإنه ينبغي تصميم سياسات لضبط وتقييد تصرفات وسلوك مصممي ومطوري الخدمات نيابة عن كل جهود بناء بيئة SOA في المجالات العامة التالية:

- **قابلية التشغيل البيئي:** لا بد من التصريح في مخطط SOA عن وسائل موحدة لتوفير التشغيل البيئي بين خدمات تقنية المعلومات. ويكون ذلك عادة من خلال مجموعة من المعايير.

- **قابلية الاكتشاف:** قد تحتاج الخدمات لسمات أو خصائص محددة كوصف سهل للعمل ومعلومات متعلقة بموقع الخدمة داخل بيان للتصنيف أو التسجيل الذي قد تم إنشاؤه

من قبل. إن هذه العناصر تجعل من الممكن اكتشاف ومعرفة الخدمات التي يمكن أن تُحدد أو تُعرف لاحقاً من خلال السياسة.

• **الأمن:** ينبغي التصريح في مخطط SOA عن وسائل موحدة لتوفير الأمن عبر جميع خدمات SOA. كما ينبغي أن يكون نمط ومعاملات هذا الأمن متسقاً مع كل الممارسات الخاصة بحوكمة أمن تقنية المعلومات في المؤسسة. كما ناقشنا في الفصل العاشر من هذا الكتاب.

• **التفرد:** لا يجب أن يكون للخدمات الجديدة أسماء الخدمات نفسها التي تم إنشاؤها من قبل. يمكن للسياسات أن تساعد في التأكد من أن المجموعات لا تواجه هذه المشكلة.

• **امتثال الواجهة:** إن طريقة استخدام وتدشين جميع الخدمات يجب أن تكون موحدة. ومع أن خدمات SOA تعد أكثر من مجرد عناصر برمجية لتقنية المعلومات، فإن هذه العملية مشابهة لأمر التشغيل Run Command الموجود في نظام ميكروسوفت ويندوز. لذا يجب أن يتم فرض هذا الشكل المعياري للواجهة عن طريق السياسة.

• **امتثال صيغ البيانات:** كما ذكرنا، يجب أن يكون الهدف الرئيسي لخدمات SOA هو إعادة استخدام عناصر الخدمات. فالطريقة الشائعة للمحافظة على هذه الميزة (إعادة الاستخدام) هي إنشاء صيغ بيانات مشتركة تُعرف بالمخططات schemas. إذ القيام بهذا العمل سيضمن إمكانية استخدام حقل العنوان التابع لإحدى الخدمات من قبل خدمة أخرى حتى لو كان هناك اختلاف في الطريقة التي تُخزن بها الخدمات بياناتها. لذا يجب أن يتم فرض المخططات المشتركة عن طريق السياسة.

• **المقاييس:** يجب أيضاً القيام بوضع معلومات وتقارير إحصائية تتعلق بقضايا تصميم الخدمة من خلال السياسة. لن تتمكن المؤسسة ولا فريق تدقيق تقنية المعلومات من قياس العمليات التشغيلية لبيئة SOA ما لم يكن هناك بعض المقاييس الموضوعة لكل من الأهداف والحد الأدنى من معايير الأداء الخاصة بالتشغيل.

يجب أن تتصل عمليات SOA خلال التصميم بصورة نمطية مع دورة حياة تطوير النظم SDLC الخاصة بالمؤسسة. وسيتم الحديث عن دورة حياة تطوير النظم وأهميتها في حوكمة تقنية المعلومات في الفصل الخامس عشر من هذا الكتاب. كما يمكن تطوير

دورة حياة تطوير خدمات مشابهة في هذه الحالة. إن اعتماد بيئة SOA يطرح تحديات بالنسبة للمؤسسات التي اعتادت استخدام تطبيقات تقنية المعلومات كوسيلة لمعالجة المتطلبات الخاصة بالتطبيقات. عادة ما يشار إلى الهياكل والعمليات الجديدة بدورة حياة SOA والتي تكون مطلوبة لتوفير الأساس للرشاقة التنظيمية وتروج لنجاح عملية اعتماد بيئة SOA. حيث أصبح دمج عمليات دورة حياة SOA مع الهياكل التنظيمية الفعالة من العناصر الرئيسية في إطلاق العمليات الفعالة لبيئة SOA.

تقع معظم أقسام تقنية المعلومات في المؤسسة تحت ضغط شديد من أجل تقديم حلول فعالة من حيث التكلفة والوقت لعمليات التشغيل الخاصة بأعمالها. ولتحقيق أهداف هذه الحلول فإن هذه الإدارات تستخدم مكونات ووحدات تقنية وتنظيمية مشتركة، هذا بالإضافة إلى استخدام المبادرات التي تتم عبر المشاريع، وذلك لتعزيز التعاون من خلال قسم تقنية المعلومات. فعندما يتم الجمع بين هذه الحلول العقلية الخاصة بتقديم الخدمات (كما هو الحال في الخدمة ذات القيمة وليس كما في التقنية)، فإنه من الممكن لإدارة تقنية المعلومات أن تجد نفسها تتحرك باتجاه الطريق المؤدي إلى بيئة SOA.

وكجزء من هذا الطريق المؤدي إلى بيئة SOA، فإنه ينبغي على جميع الأطراف سواء كانت تقنية المعلومات أو الإدارة أن يكون لديهم العقلية التي تفكر من حيث سلاسل القيمة والتي تدرك أن هذه الخدمة هي عبارة عن شيء تم إيجاده لتحقيق رضا العملاء. ومع أنه لا يمكن إنكار أن القول أسهل من التطبيق الفعال، فإن المؤسسة بحاجة إلى إنهاء التفكير التقليدي بالتطبيقات المركزية، وذلك من خلال تطبيق عمليات تنظيمية مهيكلية تتخطى حدود المشروع ودورات حياتها. عندما تتحد العقلانية والمنهجية والأشخاص والمنظمة والتقنية بشكل ناجح، عندها يمكن أن يعود تبني SOA بفوائد عظيمة على المؤسسة من حيث الحجم والفاعلية وخصوصاً الخفة والرشاقة.

سياسات وعمليات بيئة SOA خلال التشغيل:

يتضمن وقت التشغيل عملية التطوير بالكامل، والتجريب، والإنتاجية لنظم بيئة SOA. وسينتج عن سياسات الحوكمة خلال التشغيل احتكاكات سياسية أقل داخل المؤسسة نظراً

لأنها في الغالب تقيد نظم تقنية المعلومات بالنيابة عن مستهلكي خدمة SOA. بالنسبة للجزء الأكبر، فإن السياسات الخاصة بوقت التشغيل تكون موجودة للتأكد من أن الخدمات تعمل "كما ينبغي" طبقاً لتوقعات متلقي الخدمة. ويشمل هذا:

- **اتفاقيات مستوى الخدمة SLAs:** تمت مناقشة هذه الاتفاقيات في الفصل السابع عشر من هذا الكتاب. حيث يجب أن يتفق كل من مقدمي خدمات SOA ومستهلكيها على التوقعات الخاصة بالأداء طبقاً لاتفاقية مستوى الخدمة، هذا بالإضافة إلى المقاييس التي تثبت بأن الخدمات تعمل كما هو متوقع.

- **التحقق:** يجب أيضاً أن يتفق كل من مقدمي ومستهلكي الخدمات على الطريقة التي يجب اتباعها لتحديد هوية المستهلكين للتعريف عن أنفسهم. فبناءً على معايير الحوكمة الخاصة بوقت التشغيل، فإنه ينبغي أن يتضمن التحقق قضايا مثل نظم تحديد الهوية واستخدام بطاقات الأمن.

- **التصريح:** يجب أن يكون هناك عمليات أمنية معمول بها لتحديد ما إذا كان مقدم الخدمة مسموحاً له استدعاء الخدمة أم لا.

- **التشفير:** وهو جزء من العمليات القوية لأمن المعلومات. لذا يجب أن يكون هناك معايير تشفير لإبقاء الرسائل مشفرة أو مشوشة بحيث لا يمكن قراءتها بسهولة من قبل أشخاص غير مصرح لهم.

- **التنبيهات والإشعارات:** يجب وضع شروط لإطلاق التنبيهات من خلال إجراءات وذلك لإرسالها إلى المعنيين. ويمكن أن تشير التنبيهات إلى شروط خاصة بالأعمال وكذلك شروط تقنية.

- **المقاييس:** ينبغي وضع مؤشرات أداء رئيسية ومقاييس أثناء التشغيل لتوفير مؤشرات يمكن استخدامها لاحقاً لتقييم الأداء.

تقوم السياسات الخاصة بوقت التشغيل عادةً بالتشديد على الفريق المسئول عن عمليات تشغيل تقنية المعلومات ونظم تقنية المعلومات بالنيابة عن مستهلك الخدمة. حيث يمكن أن تشمل هذه العمليات طلبات الدعم الفني والاستجابة الفورية للتنبيهات

والإشعارات. ويعد تمكين طلب الاستجابة الأكثر سرعة لتغيير الشروط الخاصة بوقت التشغيل من الأمور المهمة في بيئة SOA.

تماماً كما هو الحال بالنسبة لنقاط التفتيش الجمركية الموجودة على حدود الدولة والتي تقوم بفحص كل من جواز السفر والأمتعة، فإن العملية الفعالة لحوكمة تقنية المعلومات تضع نقاط تفتيش للتأكد من أن الاتفاقيات بين الإدارات يجري تنفيذها والالتزام بها، متضمناً ذلك مستودع سجل خدمات SOA الذي يعتبر بمثابة نقطة إنفاذ لسياسات وعمليات SOA خلال وقت التصميم. لذا يجب أن يكون لدى نظام برمجيات التحكم وسائل للعمل في نقاط إنفاذ للسياسات والعمليات الخاصة بتشغيل SOA؛ متضمناً ذلك عمليات التحقق من الرسائل، وذلك لضمان التأكد من أنه مصرح لها باستدعاء الخدمة، ويعد هذا أحد المطالب التشغيلية المهمة.

لقد أكدنا أهمية اتفاقيات مستوى الخدمة SLAs في العديد من الأماكن خلال حديثنا عن عمليات بيئة SOA. حيث تقوم اتفاقيات مستوى الخدمة المعرفة جيداً والتي يتم متابعتها على نحو جيد بمراقبة صحة وأداء الخدمة وضمان تقديم الخدمات للمستهلكين كما تم الاتفاق عليه.

تتغير متطلبات وسمات بيئة SOA المشار إليها في الفقرات السابقة باستمرار أكثر بكثير من أي منطق وظيفي للخدمة. لذا يجب أن يدرك كبار المديرين أن المهمة الأساسية لحوكمة بيئة SOA هي تعزيز وضمان السلوك المرغوب فيه بين الأشخاص المشاركين والنظم. كما يجب على إدارة تقنية المعلومات الإفصاح بوضوح عن سياسات بيئة SOA الخاصة بها، ثم تقوم بعد ذلك بفرض هذه السياسات بشكل متناغم وثابت طوال دورة حياة بيئة SOA.

في الأيام الأولى لظهور SOA، كان مهندسو هذه البيئة يقضون عدة أسابيع أو حتى شهور ليقوموا بعملية التوثيق الدقيق لهذه السياسات في كتب ضخمة والتي لم يهتم أحد بقراءتها. وهذا أشبه بالخطط القديمة للتعافي من كوارث تقنية المعلومات التي أصبحت تسمى الآن خطط استمرارية تقنية المعلومات كما وضحنا في الفصل العاشر من هذا الكتاب. فإن لم تكن عملية تحفيز المشاركين على الإلمام بهذه السياسات مسألة تتسم بالصعوبة الشديدة فإن إجراء التغييرات على هذه السياسات سيكون أكثر صعوبة. فقد كانت العمليات القديمة

للمراجعة والموافقة اليدوية لازمة التطبيق لإجبار الجميع على قراءة القوانين الجديدة والالتزام بها. لكن سرعان ما أصبحت هذه المراجعات مأزقاً مما شجع الناس على الالتفاف حول هذه السياسات مما أدى إلى إبطال المهمة الرئيسية لحوكمة SOA.

في حين أن هذا الأمر ينطبق على جميع السياسات الخاصة بتقنية المعلومات، إلا أن الممارسات القوية والفعالة لإدارة سياسة SOA تعد هنا وبشكل خاص من الأمور المهمة. وعلى الرغم من المسؤوليات الحقيقية الملقاة على عاتق إدارة تقنية المعلومات، فإنه يجب التعبير عن سياسات SOA الخاصة بالمؤسسة بصيغ واضحة يمكن تعريفها وتغييرها وإزالتها بسهولة حسب الحاجة. هذا بالإضافة إلى أنه يجب أن تكون العمليات مفعلة لتقوم بإنفاذ تلك السياسات الخاصة ببيئة SOA بصورة فعالة كما هو مطبق طوال دورة حياة SOA. لذا يجب أن يتلقى المشاركون تغذية راجعة فورية من خلال إدارة السياسات التي تعتبر من العناصر الحاسمة في عمليات حوكمة SOA.

تعمل الإدارة الفعالة لسياسات SOA على إزالة العقبات والاعتراضات على حوكمة SOA، وذلك من خلال توفير دليل واضح يتعلق بما هو متوقع أن يكون متوافقاً مع المخطط الموضوع والمتفق عليه لبيئة SOA. لذا نجد أن حلول إدارة السياسات تسهم في تحسين المساءلة وضمان نتائج متناغمة.

البنية الموجهة نحو الخدمة وحوكمة تقنية المعلومات:

لقد تحدثنا عن العديد من جوانب حوكمة تقنية المعلومات المتعلقة ببيئة SOA، ولكن للأسف لم نتحدث إلا عن القليل من السمات والميزات العديدة لبيئة SOA. ففي ظل مفهوم SOA الساعي إلى فصل عناصر الوظائف البرمجية إلى مكونات مستقلة يمكن تبادلها كما يمكن ربطها أو إعادة تعريفها بسهولة، فإننا سنرى وظائف أكثر وأكثر مرتبطة بمفهوم SOA في عالمنا المتقدم المعتمد على شبكة الإنترنت. على سبيل المثال، معظم بائعي برمجيات قواعد البيانات هذه الأيام كشركة أوراكل Oracle، قاموا بتطبيق مبادئ SOA في هياكل قواعد بيانات الخاصة بتخطيط موارد المؤسسة الصادرة عنهم، كما أننا سنرى مزيداً من التركيز على SOA في منتجاتها خلال السنوات القادمة.

نكاد نجزم بأن المؤسسة التقليدية التي تستخدم مجموعة كاملة من أدوات SOA هذه الأيام لن تبدأ في البداية العمل وفقاً للنموذج الكامل لتطبيق SOA. وإنما قامت العديد من الشركات حتى اليوم بتحويل واحد أو أكثر من تطبيقاتها الرئيسية إلى نموذج خدمات الويب، وهو نهج مشابه لمفهوم SOA. وقد تم توضيح تلك العملية الخاصة بتطبيق خدمات الويب والخاصة بتحويل أحد التطبيقات الحالية إلى بيئة قائمة أو معتمدة على شبكة الإنترنت في الشكل التوضيحي (١٣-٥). كما يمكن العثور على مثال من هذا النوع من التطبيقات في واحد من الحلول البرمجية الخاصة بإدارة علاقات العملاء والمقدم من خلال شركة سيلز فورس.كوم (www.salesforce.com/company) SalesForce.com، وهي مقدم برمجيات ناجح جداً لا يبيع منتجاته البرمجية من خلال الأقراص المدمجة التي تحتوي على البرمجيات المطلوبة والمجلدات التي تحتوي على الوثائق، وإنما كل ما تقدمه شركة سيلز فورس.كوم SalesForce.com يكون في شكل ويب.

بدلاً من التطبيقات الفردية، والمستقلة، فإن تطبيقات خدمات الويب تكون مختلفة، حيث تتصل مكونات التطبيق بعضها مع بعض عبر شبكة الإنترنت، وتتصل أيضاً مكونات التطبيق مع مكونات تطبيقات أخرى باستخدام بروتوكولات الاتصالات المفتوحة. فهي عبارة عن مكونات قائمة بذاتها وتصف نفسها ويمكن استخدامها من قبل تطبيقات أخرى. وبات شبه مؤكد أن المديرين سيواجهون أعداداً متزايدة من تطبيقات خدمات الويب في المستقبل، حيث سيتم وضع العديد من الموارد المختلفة فيما نطلق عليه "سحابة" تقنية المعلومات IT Cloud، وهي بمثابة توصيلات تخزينية للعديد من الملفات ومصادر البيانات وغيرها من المواد. ويمكن للمرء أن يتطرق بفكره إلى محرك البحث جوجل، عندما ننظر في هذا المفهوم السحابي، حيث يستطيع المستخدم الحصول على واحد من العديد من نماذج البحث الناتجة بغض النظر عن مجال موضوع البحث المطلوب. وقد تكون تطبيقات خدمات الويب مرتبطة بسحابة الإنترنت تلك فضلاً عن موارد التخزين الخاصة بها مع الوصلات القائمة مع النظم المحلية، سواء كانت شبكات محلية أم لاسلكية. وقد تم الحديث في الفصل التاسع من هذا الكتاب عن المفهوم الشامل للحوسبة السحابية عندما تم تطبيقها على حوكمة تقنية المعلومات.

شكل توضيحي (١٣-٥)

نموذج تطبيقات خدمات الويب



قد تتكون بيئة SOA في المؤسسة هذه الأيام إما من بيئة نظم كاملة مطبقة بشكل كبير أو مشروع تطوير لتحويل بعض التطبيقات القائمة حالياً أو الجديدة إلى SOA. وكلاهما يواجه بعض المخاوف الرئيسية الخاصة بضوابط الحوكمة. وسيحتاج كبار المديرين الذين لديهم إلمام بالضوابط العامة لتقنية المعلومات التي تتبع نهجاً تقليدياً بشكل كبير لنظم تقنية المعلومات، إلى إعادة التفكير بتلك الأساليب المستخدمة في المراجعة. ووفقاً لمثالنا السابق حول قطع لعبة الليغو، فإننا بحاجة إلى مراجعة الضوابط وإجراءات الحوكمة المتعلقة بهذه المكونات العديدة المنفصلة، متضمناً ذلك الضوابط والصلاحيات المحيطة بكل مكون على حدة وكذلك الروابط فيما بينهم.

ربما تكون القضية الرئيسية لحوكمة تقنية المعلومات في بيئة SOA هي الحاجة إلى مخطط SOA شامل يغطي جميع عناصر الخدمات المتفق والموافق عليها من قبل الأطراف المشاركة. إن تلك الاعتبارات الخاصة بوحدة الخدمة تذهب غالباً إلى ما هو أبعد من مجرد قسم تشغيل بل إلى ما هو أبعد من المؤسسة بأكملها فقد تصل إلى مزودي أو موردي خدمات آخرين. لذا فإن هناك حاجة إلى نظام قوي للصلاحيات وإلى ضوابط بداخل كل عنصر من عناصر الخدمات. وبالعودة مرة أخرى إلى مثالنا الذي يتحدث عن قطع أو وحدات لعبة الليغو، فكل وحدة خدمية يجب اعتبارها واحدة من قطع هذه اللعبة التي ربما تكون عبارة عن مزيج من عناصر برمجية وموارد بيانات. ويجب على وحدة الأعمال أن تجعل العناصر غير المملوكة من قبل أي من هذه القطع (الوحدات الخدمية) متاحة للوحدات الأخرى من خلال عمليات إفصاح وصلاحيات واضحة. كما يجب اعتماد وظيفة مهندس SOA بدرجة ما للقيام بمراجعة تلك العناصر الخدمية ووضع القواعد والإجراءات الداعمة.

تعد الإجراءات القوية المتعلقة بأفضل الممارسات الخاصة بالبنية التحتية، والتي تحدثنا عنها في الفصل السابع من هذا الكتاب على أنها جزء من معايير الأيزو، من الأمور الأساسية في بيئة SOA. فلا تتم عملية إطلاق المنصات الخاصة ببيئة SOA عن طريق تطبيق كل شيء بأسلوب تطبيق الكل مرة واحدة. بل، سيتم إضافة أو تعديل أو حذف الخدمات والعمليات بشكل اعتيادي وعلى أساس مستمر. التحدي هنا أكثر تعقيداً بكثير من ضوابط

خاصة بمكتبة برامج مستقلة، بل ستكون المخاوف متعلقة بعنصر برمجي واحد في التطبيق. لذا ففي ظل بيئة SOA، فإن التغيرات التي تطرأ على الوحدة الخدمية التي يمكن أن تكون جزءاً من العديد من العمليات الأخرى التي ربما لا يستطيع صاحب أو مقدم الخدمة أن يفهم تماماً من هو الشخص الآخر الذي يستخدم هذه الوحدة الخدمية. وعلى ذلك فقد يكون لمشكلة التحكم بخدمة واحدة آثار على العديد من الآخرين. لذا فإن هناك حاجة إلى ضوابط قوية في الفحص والجودة.

إن العديد من الإجراءات العامة لحوكمة تقنية المعلومات التي تم الحديث عنها في فصول أخرى من هذا الكتاب يمكن تطبيقها أيضاً في بيئة SOA. على سبيل المثال، الضوابط الداخلية لإطار العمل COSO التي تمت مناقشتها في الفصل الرابع وضوابط حوكمة تقنية المعلومات الخاصة بإدارة أمن وسرية المعلومات التي تمت مناقشتها في الفصل العاشر من هذا الكتاب ملائمين تماماً في بيئة SOA. وعلى الرغم من أن هذه الضوابط الأخرى ملائمة لبيئات مختلفة، فإن الشكل التوضيحي (١٣-٦) يوجز الضوابط الخاصة بحوكمة تقنية المعلومات في بيئة SOA. إن هذه الخطوات الإجرائية تتحدث عن بيئة لم تصل المؤسسة فيها بعد إلى درجة التناغم مع بيئة SOA بنسبة ١٠٠٪، ولكنها تتحرك باتجاه بيئة SOA من خلال مشروع تطبيقي مستمر وفقاً لمخطط متفق عليه.

لقد ناقش هذا الفصل بيئة SOA كما لو كانت مجموعة خاصة من عمليات حوكمة تقنية المعلومات. ومع ذلك، فإننا عندما نقوم بتحريك نظم وعمليات تقنية المعلومات أكثر وأكثر باتجاه بيئة خدمات شبكة الويب، حيث ستصبح عمليات SOA هي المعيار وليست الاستثناء. لذا فالمديرون بحاجة إلى التفكير بنظم وعمليات تقنية المعلومات الخاصة بهم وفقاً لنموذج بيئة SOA.

شكل توضيحي (١٣-٦)

الضوابط الخاصة بحوكمة تقنية المعلومات في بيئة SOA

١. هل قامت المؤسسة بتطوير إستراتيجية شاملة لبيئة SOA تخص تقنية المعلومات وعمليات التشغيل الخاصة بأعمالها، والموافقة عليها؟
أ. إذا كانت هناك إستراتيجية معتمدة، هل تم تنفيذها بالكامل؟ أو ما مدى اكتمالها في الوقت الحالي؟ ب. إذا لم يكن هناك خطة إستراتيجية رسمية لبيئة SOA، فما الخطط المستقبلية لتنفيذ هذا الأمر؟ ج. هل توجد برامج تعليمية تم تقديمها لتوضيح فوائد بيئة SOA العائدة على كل من الأعمال ومستخدمي تقنية المعلومات؟
٢. هل تم تعيين المدير المسؤول عن قيادة وتنسيق الأعمال والجهود المبذولة في بيئة SOA في المؤسسة؟
٣. هل حصلت المؤسسة على أي من برمجيات SOA أو قامت بتقييمها؟ أ. هل تم وضع معايير تقييم رسمية لاختيار البرمجية المناسبة؟ ب. بالنسبة لأي برمجية معمول بها، هل كان هناك برنامج فحص وتقييم رسمي لتحليل المنتج البرمجي فيما يخص التطبيق الكامل؟
٤. هل تم تحديد تطبيقات "الأعمال الحساسة" على أنها جزء من إستراتيجية SOA؟ أ. بالنسبة للتطبيقات الحساسة التي لا زالت غير قائمة على خدمات شبكة الويب، هل يوجد هناك مخططات موضوعة موضع التنفيذ لتحويلها إلى بيئة SOA؟ ب. هل تم تعريف وتوثيق طبقة عمليات الأعمال الحساسة بشكل رسمي لتطبيقات بيئة SOA؟ ج. هل هناك دليل على أن طبقة خدمات التطبيقات تركز على تكامل التشغيل الداخلي، ومعتمدة على قاعدة البيانات، والمكونات، والبنية التحتية؟
٥. هل تم تكوين فريق رسمي لإدارة أو قيادة خدمات SOA؟ أ. هل تمت مراجعة الأهداف والمخاطر الخاصة بمدير الخدمة مع الإدارة؟ ب. هل تم شرح ومناقشة خطط المؤسسة الخاصة ببيئة SOA مع الأعضاء الرئيسيين في فريق الإدارة؟

٦. هل هناك دليل على أن خطط SOA متكاملة تماماً مع خطط استمرارية الأعمال في المؤسسة؟
٧. نظراً لأن المؤسسة تتجه نحو بيئة SOA، فهل تمت عملية التحويل الأولي للتطبيقات من وضعها التقليدي إلى بيئة SOA على أساس الفحص؟
أ. كجزء من أي تحول تجريبي إلى بيئة SOA، هل تمت مراجعة وتقييم ضوابط التطبيقات القائمة حالياً؟
ب. هل يشتمل أي جزء من عملية تحويل تطبيق ما إلى بيئة SOA على فحص للسمات الخاصة بمكونات "التوصيل والتشغيل" Plug and Play والتي تعد من الفوائد المفترضة للعمليات التشغيلية لبيئة SOA؟
ج. هل هناك دليل على أن التكاليف والفوائد الناجمة عن أي عملية تحويل لبيئة SOA قد تم تقييمها رسمياً؟
٨. بناء على الفحوصات والتقييمات، هل جميع التطبيقات المحولة لبيئة SOA متسقة مع المتطلبات الأمنية الخاصة بتطبيقات ونظم تقنية المعلومات المؤسسية؟
٩. على أساس الاختبارات، هل تم وضع إجراءات واستيعابها من قبل كل من تقنية المعلومات والمديرين المسؤولين عن التطبيقات المحولة إلى بيئة SOA؟
١٠. هل تم تحديد وتقييم للتكاليف والفوائد الناجمة عن أي تحويل لبيئة SOA قبل عمل أي تحويلات مخطط لها على نطاق واسع؟

ملاحظات:

١. ليجو LEGO اسم علامة تجارية لعدد كبير من عناصر البناء وأي شكل من أشكال الألعاب في أشكال وألوان مختلفة، والتي يمكن توصيلها معاً لخلق هياكل مختلفة للألعاب، ومن ثم تفكيكها بسهولة لخلق شيء آخر. هذا المنتج من ألعاب الأطفال متاح في جميع أنحاء العالم. فهو نموذج جيد للبناء من خلال تركيب المكونات. مزيد من المعلومات يمكن العثور عليها في الموقع www.LEGO.com.
٢. إطار عمل نت. (Net.) أو دوت نت عبارة عن نموذج برمجة شامل ومترابط لبناء التطبيقات. www.microsoft.com/net.
٣. بيا BEA هو أحد وحدات شركة أوراكل. يمكن العثور على معلومات عن تطبيق الويب لوجيك WebLogic الخاص به في موقع www.oracle.com/bea/index.html

الفصل الرابع عشر

إدارة تهيئة ومحفظة تقنية المعلومات

إن أي نظام تقنية معلومات مثبت، سواء كان جهاز حاسب لوحي أم حاسباً آلياً محمولاً خاصاً بأحد المديرين أو نظاماً خادماً داعماً لمكتب مبيعات أحد الفروع أو مركز بيانات رئيسياً لإحدى الشركات؛ سيكون به العديد من المكونات التي تشمل محافظ البرامج التطبيقية والملفات وقواعد البيانات ونظم التشغيل وأجهزة الاتصال ووثائق الدعم الخاصة بهذه الإجراءات. وينبغي أن تكون كل هذه المكونات مترابطة بين جميع الأنظمة وعبر المؤسسة بأكملها لكي تكون قادرة على الاتصال والعمل بعضها مع بعض. ويطلق على هذا التجميع الكامل لمكونات تقنية المعلومات اسم تهيئة تقنية المعلومات IT Configuration في المؤسسة. وكأحد العناصر الهامة في حوكمة تقنية المعلومات، فإنه ينبغي أن يكون هناك عمليات معمول بها لإدارة التوافق بين مكونات هذه التهيئة لتقنية المعلومات وحالتها كالتأكد من قدرة هذه المكونات على التحدث والتواصل معاً. لذا ينبغي على المؤسسة أن تمتلك نظاماً فعالاً لإدارة تهيئة تقنية المعلومات، وذلك لدعم عمليات تقنية المعلومات الرئيسية لديها.

يتعرض مديرو الأعمال غالباً إلى مسائل تتعلق بتهيئة تقنية المعلومات عندما يتلقون بلاغاً أو رسالة خطأ من إحدى إدارات المؤسسة التابعين لها ويكتشفوا أنه ليس بإمكانهم قراءة الملف الذي تم إرساله. وتكون أول ردة فعل للمدير الاتصال بفريق الدعم الفني التابع لإدارة تقنية المعلومات التابعة له أو لها، وفي الغالب يتم تتبع المشكلة لنكتشف أن الوحدة التي قامت بإرسال البيانات التي لا يمكن قراءتها قد قامت باستخدام أحد الإصدارات الخاطئة للبرمجية أو حتى أنها قد استخدمت برمجية غير صحيحة بالمجمل. وفي الغالب يكون سبب مشكلة تلك البرمجية الخاطئة أو غير القابلة للقراءة هو الإخفاق في تحديث أحد عناصر البرمجية في مكان ما في شبكة تقنية المعلومات الخاصة بالشركة. فقد يكون التقرير أو العملية جيداً في الموقع الذي يتم تشغيلها فيه حالياً، ولكنها غير متوافقة مع نظم وأجهزة أخرى. ويعد هذا أحد الأمثلة على المشاكل المتعلقة بتهيئة تقنية المعلومات!

هناك حاجة للمحافظة على إعدادات ثابتة ومتوافقة بين الموارد الخاصة بتقنية المعلومات، سواء كانت ملفات بيانات وبرامج محملة على جهاز حاسب شخصي محمول أو على موارد موجودة في مكان ما في شبكة تقنية المعلومات الخاصة بالشركة. إذا حدث تغيير أو تعديل على أحد المكونات يكون هناك غالباً حاجة لانعكاس ذلك على جميع المكونات الأخرى المترابطة معه. وتُعرف الإدارة الخاصة بمراجعات تلك العناصر العديدة لتقنية المعلومات وإصداراتها باسم إدارة تهيئة تقنية المعلومات IT configuration management. وينظر إلى هذا المجال غالباً على أنه مجرد رقابة فنية فقط على تقنية المعلومات، في حين أنه يجب أن ينظر للإدارة الفعالة لتهيئة تقنية المعلومات على أنها أحد المكونات الهامة والضرورية لحوكمة تقنية المعلومات.

يناقش هذا الفصل أهمية عمليات إدارة تهيئة تقنية المعلومات في كل المؤسسات ويوجز الأدوات الرئيسية لحوكمة تقنية المعلومات اللازمة لإيجاد نظام فعال لإدارة التهيئة الخاصة بالمؤسسة Configuration Management System (CMS) مع التركيز على إنشاء ما يسمى قاعدة بيانات إدارة التهيئة Configuration Management Database (CMDB). وقد تم تسليط الضوء على بعض عناصر عمليات إدارة تقنية المعلومات في الفصل السادس من هذا الكتاب الذي كان يدور حول أفضل الممارسات الخاصة بآيتل وإدارة خدمات تقنية المعلومات، إلا أن هذا الفصل يؤكد مرة أخرى أهمية إدارة تهيئة تقنية المعلومات بوصفها أحد الضوابط الهامة لحوكمة تقنية المعلومات.

كما سيقدم ويناقش هذا الفصل أيضاً إدارة محفظة تقنية المعلومات على أنه أحد المفاهيم الهامة في حوكمة تقنية المعلومات. وكما هو الحال بالنسبة للعديد من الأفراد الذين يستثمرون في أحد صناديق الاستثمار التعاونية أو في أحد صناديق التداولات التجارية للبورصة الذي يحتوي على محفظة أوراق الاستثمار المالية ذات العلاقة، فهناك مزايا قوية لحوكمة تقنية المعلومات نتيجة إدارة موارد تقنية المعلومات، وذلك استناداً إلى مجموعات أو محافظ التطبيقات والبنية التحتية والمشاريع وموارد تقنية المعلومات ذات الصلة. وسوف نصف هنا كيف يمكن لنهج إدارة محفظة تقنية المعلومات الخاصة باستثمارات تقنية المعلومات أن يؤدي إلى العديد من الفوائد لصالح إدارة تقنية المعلومات والمؤسسة بأكملها. وتعتبر إدارة محفظة تقنية المعلومات واحدة من الطرق الفعالة لإدارة استثمارات

تقنية المعلومات والتي يمكن أن توفر رقابة مركزية على ميزانيات تقنية المعلومات وقضايا إدارة مخاطر تقنية المعلومات والتوافق الإستراتيجي لاستثمارات تقنية المعلومات. فإدارة محفظة تقنية المعلومات تسهم في دعم ممارسات محسنة لحوكمة تقنية المعلومات.

مفاهيم إدارة تهيئة تقنية المعلومات:

يوجد العديد من المعدات والبرمجيات ومكونات البنى التحتية الخاصة بتقنية المعلومات في أي نظام من أنظمة تقنية المعلومات المؤسسية. وهي تمتد من خادم قواعد بيانات مع مجموعة من الأجهزة الطرفية المتصلة به والتي تستطيع أن تخدم وحدة أعمال صغيرة وصولاً إلى مجموعة كبيرة من عمليات تشغيل تقنية المعلومات على مستوى الشركة والتي تخدم مرافق مختلفة في جميع أنحاء العالم. بعض هذه المكونات تكون مترابطة فيما بينها، في حين أن البعض الآخر يكون قائماً بذاته ومنفصلاً عن باقي المكونات. إن تهيئة تقنية المعلومات في المؤسسة تعد أكثر من مجرد قائمة من المكونات البرمجية والأجهزة والمعدات المثبتة. بل يجب على السجلات الخاصة بالتهيئة أن تحتفظ بأمور مثل روابط الواجهة والتعريفات الخاصة بإصدار المكون والخصائص المثبتة وجميع الأمور الأخرى التي تصف تلك العناصر والبنود الخاصة بتهيئة تقنية المعلومات في الحالات التي تم تثبيتها فيها.

لقد تطرقنا سابقاً إلى مفاهيم إدارة تهيئة تقنية المعلومات في الفصل السادس من هذا الكتاب والذي يدور حول إطار العمل آيتل والمفاهيم الخاصة بإدارة خدمات تقنية المعلومات. كانت إدارة تهيئة تقنية المعلومات هناك عبارة عن عنصر واحد فقط من بين سلسلة من الممارسات الجيدة للإطار آيتل. في حين أن هذا الفصل ينظر بعمق أكبر بقليل إلى أدوات وعمليات إدارة تهيئة تقنية المعلومات. وسيوضح هذا الفصل لماذا تعد إدارة تهيئة تقنية المعلومات أحد المكونات الهامة للعمليات الرشيدة لحوكمة تقنية المعلومات.

وعلى الرغم من عدم وجود أي تعريف موحد أو متفق عليه لنظام إدارة تهيئة تقنية المعلومات، حتى إن البحث عن طريق شبكة الإنترنت سوف يعطي أيضاً العديد من التعريفات المختلفة، فإن المنظمة التقنية لوضع المعايير والتي مقرها الولايات المتحدة، وهي IEEE، تعد من المصادر الجيدة للحصول على مثل هذا التعريف. وقد كانت هذه المنظمة

تُعرف سابقاً باسم جمعية مهندسي الكهرباء والإلكترونيات Institute for Electrical and Electronic Engineering. ويشار إليها حالياً باستخدام الأحرف الأولى من اسمها حيث أصبح الاسم الدارج لها هو IEEE "آي تريبل إي". حتى الموقع الخاص بهذه المنظمة www.ieee.org لا يشير إلى الاسم الأصلي الكامل لها. وتُعرف منظمة IEEE إدارة تهيئة تقنية المعلومات على أنها إحدى العمليات الخاصة بالمؤسسة أو بإدارة تقنية المعلومات، حيث تحتوي هذه العملية على العناصر التالية:

- **التعريف:** تشتمل عملية إدارة تهيئة تقنية المعلومات على مخطط تعريفي قوي يعكس بنية جميع موارد تقنية المعلومات، ويحدد مكوناتها وتاريخ التعديل وأنواع هذه الموارد. الأمر الذي يجعل هذه الموارد مميزة ويمكن الوصول إليها بشكل أو بآخر.
- **التحكم:** يتعين على نظام إدارة تهيئة تقنية المعلومات التحكم في الإصدارات الخاصة بجميع المنتجات والتغيرات التي تحدث على الموارد الخاصة بالتهيئة طوال دورة حياتها من خلال وجود ضوابط معمول بها تضمن تناغم الموارد الخاصة بمكونات تقنية المعلومات من خلال وضع ما يعرف بمنتجات الخط المرجعي baseline products.
- **تدوين الحالة:** يجب على نظام إدارة تهيئة تقنية المعلومات أن يسجل ويبلغ عن حالة كل مكون من مكونات بنية تقنية المعلومات وطلبات التغيير، وذلك أثناء جمع المعلومات الإحصائية الحيوية المتعلقة بتلك المكونات الموجودة في منتجات التهيئة.
- **التدقيق والمراجعة:** ينبغي أن تكون هناك عمليات مراجعة معمول بها تقوم بها إدارة تهيئة تقنية المعلومات للتحقق من سلامة اكتمال جميع بنود تهيئة تقنية المعلومات والحفاظ على التوافق فيما بين المكونات المترابطة بداخل التهيئة من خلال ضمان أن هذه المنتجات هي عبارة عن مجموعة من المكونات المعرفة على نحو جيد.

سوف تناقش الفقرات التالية تلك العناصر الخاصة بإدارة تهيئة تقنية المعلومات ونظام إدارة التهيئة CMS بمزيد من التفصيل. فللوصول إلى إدارة فعالة لتهيئة تقنية المعلومات، فإنه يتعين على المؤسسة وإدارة تقنية المعلومات التابعة لها (١) امتلاك عمليات معمول بها لتحديد جميع المكونات الخاصة بالأجهزة والبرمجيات والبنية التحتية، والتي تعد جزءاً من موارد تقنية المعلومات لديها. (٢) امتلاك ضوابط معمول بها لمتابعة كل التغيرات

والتنقيحات التي تتم على هذه المكونات الخاصة بتهيئة تقنية المعلومات. (٣) الإبقاء على نظام تبليغ خاص بإدارة التهيئة بحيث يكون كل من إدارة تقنية المعلومات والإدارة العامة والموارد المالية على دراية بالوضع الراهن لموارد تقنية المعلومات الخاصة بالمؤسسة. (٤) متابعة وإدارة حالة تلك الموارد الخاصة بتقنية المعلومات للتأكد من أنها قائمة، وفعالة من حيث التكلفة.

إن الإدارة الفعالة لتهيئة تقنية المعلومات هي أكثر بكثير من مجرد التحكم بإصدارات البرامج الخاصة بتقنية المعلومات من خلال قاعدة بيانات واحدة وشاملة لإدارة التهيئة CMDB، بل قد تشمل أيضاً موارد أخرى ذات صلة موجودة في أحد المرافق كإدارة تقنية المعلومات الموجودة في المقر الرئيسي للمؤسسة. كما يجب أن تشمل عمليات إدارة تهيئة تقنية المعلومات كامل المؤسسة متضمناً ذلك أي مرفق قد تكون هناك حاجة للاتصال به أو مشاركة البيانات والمعلومات معه.

لقد تحدثنا عن الممارسات الخاصة بإدارة تهيئة تقنية المعلومات التي تعد جزءاً من الإطار آيتل والذي سبق الحديث عنه في الفصل السادس من هذا الكتاب. ولأن أفضل الممارسات الخاصة بالإطار آيتل تغطي مجموعة كبيرة من المجالات، يجب إعطاء المزيد من الاهتمام بإرشاداتها المتعلقة بإدارة تهيئة تقنية المعلومات. تقدم الأجزاء القادمة من هذا الفصل المزيد من الإرشادات فيما يتعلق ببناء العمليات الخاصة بتهيئة تقنية المعلومات. يصف الشكل التوضيحي (١٤-١) هذا المفهوم الخاص بإدارة التهيئة CMS كما يصف الحاجة إلى ضوابط خاصة بتهيئة تقنية المعلومات. يعرض الرسم البياني مستخدمي نظم الأعمال المؤسسية في الإطار الدائري الخارجي له، حيث إن جميعهم بحاجة إلى إيجاد علاقات وروابط فيما بينهم من خلال موارد النظم الخاصة بهم. ويهتم هؤلاء المستخدمون للنظم بالقضايا الآتية والمتعلقة بتهيئة تقنية المعلومات:

• **ضوابط أصول تقنية المعلومات:** قد تعتمد المجموعات المختلفة للمستخدمين وإدارات تقنية المعلومات إلى شراء وتثبيت إصدارات مختلفة بعض الشيء من البرمجيات والأدوات. وفي بعض الأحيان تكون الاختلافات بشكل عام قليلة، فمثلاً قد يكون لدى إحدى الوحدات خارج البلاد إصدار مختلف بعض الشيء بسبب اختلافات اللغة. على كل حال،

قد تختلف الطريقة التي تفسر فيها البرمجية الأوامر وتتفاعل من خلالها مع إصدارات اللغات الأخرى. وقد تثير الكيفية التي تقوم من خلالها المؤسسة ووحدات العمليات التشغيلية التابعة لها بشراء وتثبيت البرمجيات والأصول الأخرى لتقنية المعلومات بعض القضايا المتعلقة بعملية التهيئة.

• **إدارة الحوادث:** إن الهدف الأول لعملية إدارة الحوادث هو استعادة عملية التشغيل الطبيعية للخدمة بأقصى سرعة ممكنة وتقليل التأثير على العمليات التشغيلية للأعمال. هذا من شأنه أن يضمن الإبقاء على أفضل المستويات الممكنة فيما يتعلق بجودة الخدمة وإتاحتها. من ناحية أخرى، قد تغفل النشاطات التصحيحية للحوادث الطارئة عن روابط أو اتصالات في التهيئة، مسببة بذلك مشاكل عامة على المدى التشغيلي البعيد.

• **إدارة مشاكل تقنية المعلومات:** يُعرّف الإطار آيتل المشكلة على أنها حالة يتم تحديدها غالباً نتيجة لحوادث متعددة تُظهر أعراضاً مشتركة. فعندما يتعرض أكثر من نظام أو مجموعة مستخدمين للمشكلة التقنية نفسها، فإن هناك حاجة للوصول إلى المصدر الرئيسي المسبب للمشكلة وتحديد الحل المناسب لها. فقد يصبح هذا أحد المشاكل الكبيرة في التهيئة في البيئات الكبيرة والمعقدة لتقنية المعلومات.

• **القضايا الشاملة لحوكمة تقنية المعلومات:** لقد تم تغطية مجموعة واسعة من قضايا حوكمة تقنية المعلومات خلال فصول هذا الكتاب، والتي تشمل السياسات الأمنية في تقنية المعلومات وقضايا إدارة المشاريع والمقاييس المعيارية وغيرها. لذا يجب أن يتم تنفيذ وإدارة كل هذه الأمور بشكل متناغم عبر المؤسسة لضمان إدارة متسقة وفعالة للتهيئة.

• **إدارة سعة تقنية المعلومات:** تحتاج المؤسسة إلى تثبيت وتنفيذ المستويات والأحمال الصحيحة لموارد تقنية المعلومات. لذا فإن معالجة احتياجات وأحجام الخدمات بحاجة إلى متابعة وضبط عبر جميع موارد تقنية المعلومات في المؤسسة.

• **اتفاقيات مستوى الخدمة SLAs:** التي تم تقديمها مع قضايا حوكمة تقنية المعلومات التي تمت مناقشتها في الفصل السابع عشر من هذا الكتاب. هي عبارة عن اتفاقيات غير رسمية تعقدها إدارة تقنية المعلومات مع كل من مجتمعات المستخدمين التابعين

لها والموردين الخارجيين. أبسط صور هذه الاتفاقيات، أن تقوم إدارة تقنية المعلومات بوضع اتفاقية لمستوى الخدمة مع قسم المراقبة المالية بحيث يتعهد المحاسبون بتسليم جميع معاملات إغلاق نهاية الشهر الخاصة بدفتر الأستاذ العام وفقاً لجدول زمني متفق عليه على أن تتعهد إدارة تقنية المعلومات باستكمال وتسليم تقارير الإغلاق الشهرية في تاريخ محدد. من ناحية أخرى عندما تحتاج جميع الإدارات المختلفة إلى المستخدمين ومرافق تقنية المعلومات لاتفاقيات مستوى خدمة خاصة بها، قد تكون هناك مشاكل في نظام إدارة التهيئة CMS.

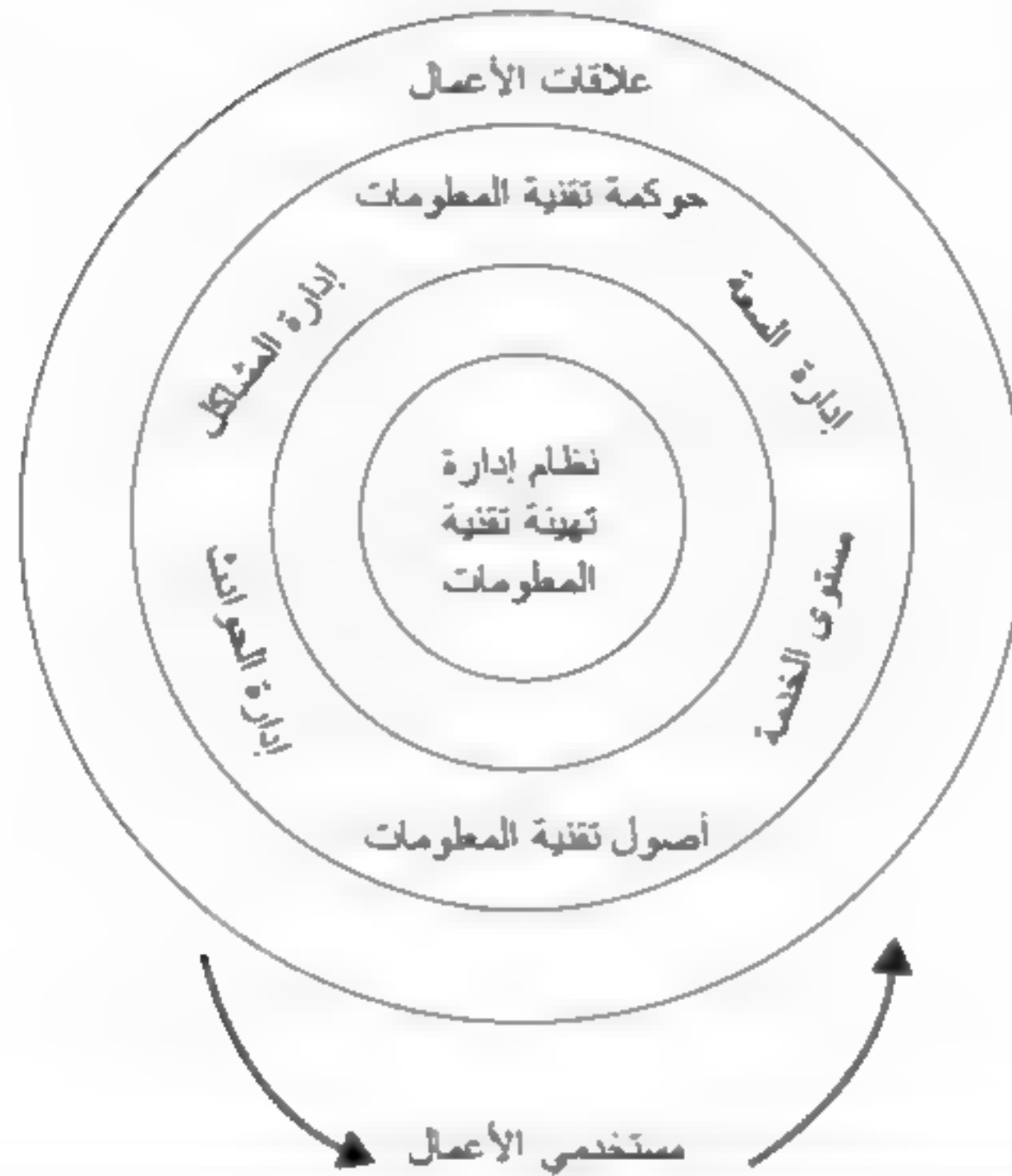
الفكرة هنا هو أننا يجب أن ننظر إلى إدارة تهيئة تقنية المعلومات على أنها مجموعة من المفاهيم التي تكون منفصلة غالباً لكنها مترابطة (انظر الشكل التوضيحي ١٤-١). ويعد هذا من الأمور الهامة خصوصاً هذه الأيام؛ إذ إننا قد ابتعدنا كثيراً عن الحاسبات المركزية التي كانت موجودة في الماضي وقمنا بتثبيت أشكال وأنواع عديدة من موارد تقنية المعلومات في المؤسسة التقليدية ذات الوحدات والمواقع المتعددة. وبينما يجب على الإدارة التقليدية لتقنية المعلومات أن تضع معايير على ما تمتلكه (نظم وعمليات تقنية المعلومات) وكذلك على نظم وعمليات تقنية المعلومات الخاصة بالمقر الرئيسي، فإننا نجد أن ضوابط التهيئة قد تضيع في عالم النظم اللاسلكية المتصلة بالنظم السحابية.

أفضل ممارسات إطار آيتل الخاصة بإدارة تهيئة تقنية المعلومات:

قدم الفصل السادس من هذا الكتاب المواد الخاصة بمكتبة البنية التحتية لتقنية المعلومات ITIL فيما يتعلق بالحوكمة، وقد تم هناك عرض أفضل الممارسات بالشكل التوضيحي (٦-٢) موضحاً أهمية إدارة التهيئة على أنها إحدى أدوات حوكمة تقنية المعلومات. الفكرة هي أن كل مؤسسة تمتلك أو تحتفظ بعناصر متنوعة من المعلومات عن البنية التحتية الخاصة بتقنية المعلومات لديها، فضلاً عن أن المؤسسة، تواجه تحدياً بالنسبة لعملية الحفاظ على النسخة الأخيرة المحدثة لجميع هذه المعلومات. وقد حددت إدارة التهيئة في الإطار آيتل أفضل الممارسات للاحتفاظ بتفاصيل المعلومات الموثوقة والحديثة المتعلقة بالبنية التحتية لتقنية المعلومات.

شكل توضيحي (١٤-١)

مفاهيم نظام إدارة تهيئة تقنية المعلومات



مع أن هذا المصطلح لا يعد من المصطلحات الشائعة الاستخدام بالنسبة للعمليات التشغيلية الخاصة بتقنية المعلومات هذه الأيام، فإن إطار العمل آيتل يدعو المؤسسة والعمليات التشغيلية الخاصة بها إلى تعريف هيكل التهيئة الخاص بها إلى ما يطلق عليه الإطار آيتل عناصر التهيئة (CIs)، كما يدعو الإطار آيتل أيضاً إلى أن نفهم كيف ترتبط عناصر التهيئة CIs هذه بعضها مع بعض. كما يجب على العملية الفعالة لإدارة التهيئة في آيتل أن تؤكد أن التغيرات التي حدثت على بنية تقنية المعلومات قد تم تسجيلها بشكل صحيح، بما فيها العلاقات بين عناصر التهيئة CIs. كما يجب على عملية إدارة التهيئة مراقبة حالة مكونات تقنية المعلومات لضمان أنها تملك الوصف الدقيق للإصدار الحالي لتلك العناصر CIs.

وفي خطوة أولى لبناء عمليات التهيئة الفعالة لتقنية المعلومات، فإن المؤسسة تحتاج إلى القيام بجرد موارد تقنية المعلومات الموجودة لديها. فهذه العملية تحتاج إلى ما هو أكثر من

مجرد مسح لقوائم المكونات البرمجية المثبتة وعمل الجرد المادي لمعدات تقنية المعلومات الموجودة على الأرض. يحتوي الشكل التوضيحي (٢-١٤) على قائمة بأنواع الموارد التي يجب أن تصبح من عناصر التهيئة CIs لتحديد بيئة التهيئة، ومثابة اللبنة الأولى في قاعدة بيانات إدارة التهيئة CMDB كما سيتم مناقشته في الأجزاء اللاحقة. وعند تنفيذ الجرد بصورة فعالة، فإنه يجب أن يُزوّد هذا الجرد كلاً من الإدارة وإدارة تقنية المعلومات بالمعلومات والمجالات لمزيد من التحقيق في المجالات التالية والخاصة بسياسة منتجات تقنية المعلومات:

- ما مكونات تقنية المعلومات المستخدمة حالياً؟ وكم عدد الإصدارات المختلفة المعمول بها لكل مكون؟ وما المدة التي استخدمت فيها هذه المكونات؟
- ما المكونات التي يمكن أن يتم سحبها تدريجياً؟ وما المكونات التي تحتاج إلى تعديل؟
- ما التراخيص المفعله؟ وهل هي كافية؟
- ما مدى معيارية البنية التحتية الشاملة لتقنية المعلومات عبر المؤسسة؟

شكل توضيحي (٢-١٤)

أمثلة على عناصر التهيئة الموجودة في قاعدة بيانات إدارة التهيئة CMDB

• جميع منصات الحوسبة المادية وتشمل أجهزة الحاسب المكتبي والحاسب المحمول والخوادم المثبتة على حامل rack-mounted والخوادم النخيفة Blade servers وأجهزة أخرى قائمة بذاتها.
• جميع أجهزة ومعدات الشبكة متضمنة الطابعات المتصلة بالشبكة.
• جميع التطبيقات والبرامج الخدمية Utilities الخاصة بالبرمجيات الوسيطة Middleware والبرمجيات Software متضمنة المنتجات الخاصة بالمستخدم النهائي، والإدارة والدعم.
• جميع نظم التشغيل المثبتة وكذلك أدوات حزم تطوير البرمجيات مثل جافا JAVA وسي شارب C# وأدوات البرمجيات الإدارية الخاصة بدورة حياة تطوير النظم SDLC.
• تنصيبات الرقع Patches الخاصة بأنظمة التشغيل وأجهزة الشبكة.
• شبكة الهواتف المحلية Private Branch Exchange (PBX) ومعدات وبرمجيات الاتصالات المتعلقة بها.
• خدمات الأعمال المثبتة أو عناصر هذه الخدمات.
• حزم الوثائق الخاصة بالتطبيقات والنظم والمعايير الخاصة بالسياسات والعمليات.

الفكرة هنا هي أن المفاهيم الخاصة بإدارة تهيئة تقنية المعلومات ونظام إدارة التهيئة CMS لا يجب أن تكون مجرد قضايا تابعة لإدارة تقنية المعلومات في المؤسسة. بل يجب تشكيل فريق مكون من المختصين في التقنية يشمل إدارة تقنية المعلومات وغيرهم من المستخدمين الرئيسيين لموارد تقنية المعلومات من أجل بناء وتشيد نظام لإدارة التهيئة CMS في المؤسسة. لذا يجب إعطاء المزيد من الاهتمام من أجل ضم أعضاء لفريق مشروع نظام إدارة التهيئة CMS من أشخاص في المؤسسة لا علاقة لهم بتقنية المعلومات والذين يستخدمون الموارد الأخرى عادة للنظم ولديهم اتصالات محدودة مع نظم المؤسسة الأكثر مركزية. كما يجب أن يحتوي النظام الفعال لإدارة التهيئة على كل مجموعات المعلومات المشار إليها في الشكل.

جمع وتحليل متطلبات إدارة التهيئة:

بينما يدرك العديد من المديرين والعاملين في تقنية المعلومات أهمية امتلاك عمليات خاصة بتهيئة فعالة لتقنية المعلومات ومعمول بها في المؤسسة؛ قد تمثل عملية جمع وتحديد المتطلبات الضرورية للبدء بإدارة التهيئة على مستوى المؤسسة بشكل دقيق ومحدد، أحد التحديات الموجودة. حيث يجب أن تبدأ هذه الممارسة من خلال النظر إلى أدوات التهيئة المعمول بها، وإجراء التعديلات اللازمة عليها حسب الحاجة، ومن ثم بناء علاقات رفيعة المستوى لإدارة التهيئة بحيث تحمل توقعات أكثر واقعية والانتقال إلى متطلبات قابلة للقياس لعملية تهيئة تقنية المعلومات.

إن هذه العملية الخاصة ببناء وإطلاق مكونات إدارة تهيئة تقنية المعلومات وتحديد متطلباتها الضرورية يجب أن تبدأ عادة بالتخطيط ومنح التصاريح وإطلاق مشروع رسمي لتطوير نظم تقنية المعلومات، وذلك وفقاً لمبادئ حوكمة إدارة المشاريع التي سنتحدث عنها في الفصل السادس عشر من هذا الكتاب، فالممارسات القوية لإدارة المشاريع تعد من الأدوات المهمة لإطلاق عملية فعالة لإدارة التهيئة. ويجب أن يتضمن مشروع إدارة تهيئة تقنية المعلومات العناصر الأربعة التالية:

١- تحديد عناصر تهيئة تقنية المعلومات: تتطلب هذه الخطوة وضع تعريف شامل لنطاق التهيئة وبيان قائمة بعناصر التهيئة كالموضح بالشكل التوضيحي (١٤-٢)، وكذلك وضع تعريف شامل لعملية تعقب التغيرات، وذلك لإدارة عناصر التهيئة في بيئة تقنية المعلومات.

٢- بناء العلاقات الخاصة بتهيئة تقنية المعلومات: يجب ربط عناصر التهيئة CIs المختلفة تلك مع تقنية المعلومات وعمليات الأعمال.

٣- تحسين عمليات تهيئة تقنية المعلومات: ربما يجد فريق المشروع أن هناك العديد من عناصر التهيئة CIs مكررة بشكل أساسي بعضها من بعض. ولكن كل عنصر منها موجود في نظام أو قاعدة بيانات مختلفة. لذا يجب بذل المزيد من الجهد لتبسيط وتنفيذ هذه العمليات. على سبيل المثال، يجب أن يتم حفظ أرقام دفتر الأستاذ العام للنظام المحاسبي في مكان واحد فقط. فالاحتفاظ بقائمة في أماكن متعددة من شأنه أن يقود فقط إلى أخطاء أو مشاكل أخرى ستأتي لاحقاً.

٤- إيجاد عمليات توثيق متسقة لإدارة تهيئة تقنية المعلومات: ويعد هذا الأمر أحد المعايير الهامة في الحوكمة والتي كانت جزءاً من نقاشنا الدائر حول حوكمة تقنية المعلومات في العديد من الفصول.

إن هذه العملية الشاملة لإدارة التهيئة تشبه إلى حد ما أي عملية يجب توظيفها عند الحاجة لتنظيم مجموعة كبيرة من عناصر المعلومات المختلفة والمتراصة في الوقت نفسه، مع الحاجة إلى أن نكون قادرين على أن نشير إلى تلك العناصر بانتظام وأن نطبق التغيرات عليها حسب الطلب. ففي حين أن السجلات الشخصية، مثل السجلات الخاصة بإيصالات الضريبة على دخول الأفراد أو سجلات المنتجات وقطع الغيار الخاصة بتجار التجزئة يتم تنظيمها عادة ولو على الأقل بصورة غير رسمية شكل من أشكال التهيئة، نجد أن العديد من إدارات تقنية المعلومات تفتقر إلى وجود هذه الأنواع من التطبيقات. فهم يقومون بتثبيت نظم وبرمجيات جديدة، ويعتمدون غالباً على الباعة لتزويدهم بمستوى بسيط من التحكم بالتعديل أو التغيير ولكنهم لا يملكون عمليات معمول بها لإدارة تهيئة تقنية المعلومات.

يتعين على إدارة تقنية المعلومات في المؤسسة اتخاذ الخطوات اللازمة لتطبيق إدارة التهيئة على أنها مكون أساسي لجميع العمليات التشغيلية لتقنية المعلومات. فمثل هذا العمل قد يجبر تقنية المعلومات على التراجع عن بعض المشاريع العادية الأخرى، غير أن العملية الفعالة ستعود بالفوائد على كل من تقنية المعلومات ومستخدمي خدمات تقنية المعلومات.

خطوات تطبيق إدارة تهيئة تقنية المعلومات:

ينبغي على إدارة تقنية المعلومات أن تقوم بوضع معايير بشأن إصدارات البرمجيات والمعدات الخاصة بها. فالتحكم بالإصدار يكون كمنهجية تهدف إلى نشر إصدارات برمجيات متوافقة على الأجهزة المتشابهة داخل الشبكة. حيث سيسهم ذلك في تحسين فرصة التحقق من صلاحية إصدارات البرمجيات المختارة واختبارها وسيحد بشكل كبير من حجم العيوب في البرمجيات ومشكلات التوافق الموجودة على الشبكة. إن الإصدارات المحدودة للبرمجيات من شأنها أيضاً أن تقلل من مخاطر السلوك غير المتوقع، وذلك من خلال واجهات المستخدم، والأوامر أو مخرجات الإدارة، وأسلوب الترقية وسلوك الخصائص. هذا يجعل من البيئة أقل تعقيداً ويجعل عملية تقديم الدعم لها أكثر سهولة. بشكل عام، فإن ضبط إصدار البرمجيات يحسن من إتاحة الشبكات ويقلل من تكاليف الدعم التفاعلي.

إن الحديث عن التحكم بإصدارات مكونات تقنية المعلومات أسهل من القيام به فعلاً. لذا يتعين على العمليات التشغيلية لتقنية المعلومات في المؤسسة و فرق البرمجيات المسؤولية عنها أن تقوم بتعريف وتحديد تصنيفات للأجهزة اعتماداً على أنواعها ومدى ثباتها ومتطلبات إصدار مزايا جديدة. في المؤسسات الكبيرة المتعددة الإدارات، لا بد من تثبيت إصدارات برمجيات منفصلة على الأجهزة المتشابهة. هنا في الغالب يمكن التغاضي عن المعايير. فقد يكون القسم الغربي لمؤسسة ما على سبيل المثال قد نسي أن يثبت بعض التعديلات الطفيفة على النظم في حين قام القسم الشرقي من المؤسسة بتثبيتها. فعلى الرغم من أن النتائج قد تبدو متشابهة، فإن المسائل يمكن أن تُنسى إلى أن تتسبب إحدى قضايا النظم بمشاكل مستقبلاً.

ولإيجاد ضوابط فعالة لإدارة تهيئة تقنية المعلومات، فإنه ينبغي على أخصائي البرمجيات أن يقوموا باختبار إصدارات البرمجيات والتحقق من صلاحياتها وتجربتها. وتتضمن الخطوات التالية عملية توثيق الإصدارات الناجحة كمعايير موحدة لتصنيفات الأجهزة المتشابهة. الفكرة هنا هي نشر وترقية جميع الأجهزة المتشابهة بشكل متناغم باستخدام إصدار معياري موحد من البرمجيات.

يعد نظام إدارة تهيئة تقنية المعلومات أحد العناصر الأساسية في الحوكمة الفعالة لتقنية المعلومات. ففي الواقع لن نتمكن من إدارة جميع موارد تقنية المعلومات الخاصة بنا والتحكم فيها حتى ندرك كيف تتأقلم وتتناسب هذه الموارد معاً. إن العنصر الرئيسي في كل هذا هو الحاجة إلى إيجاد معايير وإجراءات في جميع أنحاء المؤسسة كأن يكون لدى إدارة تقنية المعلومات في المؤسسة فهم وإدراك جيد لجميع موارد تقنية المعلومات المثبتة فيها وأنه يجب أن تكون هذه الموارد مرتبطة فيما بينها وأن يتم استخدامها بشكل متناغم ومتوافق عبر المؤسسة. إن التطبيق الفعال لكل من إطار العمل آيتل الذي تمت مناقشته في الفصل السادس من هذا الكتاب، وبيان الخدمات الذي تم الحديث عنه في الفصل الثاني عشر من هذا الكتاب، سوف يساهم في تحقيق الوصول إلى هذه البيئة. من ناحية أخرى، فإن أحد العناصر الهامة في عملية التطبيق الفعال لإدارة البنية هو تطبيق قاعدة بيانات إدارة التهيئة CMDB التي تعد بمثابة المكون والمستودع المركزي لعمليات إدارة تهيئة تقنية المعلومات.

قاعدة بيانات إدارة التهيئة (CMDB): يكون غالباً مفهوماً صعباً:

قاعدة بيانات إدارة التهيئة هي عبارة عن قاعدة بيانات مفردة تحتوي على كل المعلومات المتعلقة بمكونات نظام المعلومات المستخدم في خدمات تقنية المعلومات الخاصة بالمؤسسة. بالإضافة إلى العلاقات الموجودة بين هذه المكونات. تقدم قاعدة بيانات إدارة التهيئة CMDB عرضاً منظماً للبيانات، كما توفر وسائل لفحص هذه البيانات من أي منظور نريده. ومن خلال هذا السياق فإن مكونات نظام المعلومات هذا والخاص بقاعدة بيانات إدارة التهيئة تحتوي على عناصر تهيئة مترابطة وذات مرجعية كما هو موضح في الشكل التوضيحي (١٤-٢). إن عنصر التهيئة CI قد يكون أي مكون يمكن تصويره من مكونات تقنية المعلومات متضمناً ذلك البرمجيات والمعدات والوثائق والموظفين المسؤولين، بالإضافة إلى أي مجموعة مؤلفة منهم. تسعى عمليات إدارة التهيئة إلى تحديد وضبط وتتبع عناصر التهيئة والتغيرات التي تحدث عليها بطريقة شاملة ونظامية.

يقدم العديد من كبار باعة البرمجيات منتجات برمجية مختلفة لقاعدة بيانات إدارة المحتوى CMDB. يقدم الشكل التوضيحي (٣-١٤) عرضاً تصويرياً لما يجب أن تظهر عليه قاعدة البيانات تلك أو مكوناتها الرئيسية. ليس الهدف من هذا الفصل هو تقديم وصف تقني حول كيفية اختيار وبناء قاعدة بيانات إدارة التهيئة CMDB، ولكن الهدف هو وصف المكونات الرئيسية لها. وبناءً على الشكل التوضيحي (٣-١٤) فإن قاعدة بيانات إدارة التهيئة يجب أن تحتوي على العناصر والمكونات التالية:

- **إدارة مستخدمي قاعدة بيانات إدارة التهيئة CMDB:** باعتبارها أحد النشاطات المؤسسية الرئيسية للتحكم بقاعدة البيانات، فإن هناك حاجة إلى وجود واجهة للمستخدم والمهام الإدارية. حيث سيكون هذا مزيجاً من الموارد التقنية الخاصة بتقنية المعلومات للمساعدة من خلال الإدارة والمتابعة الشاملة لقاعدة البيانات. هذا بالإضافة إلى توفير عمليات إدارية لتعريف وإدخال عناصر تهيئة CIs جديدة كلما زاد نمو وتغير النظم والعمليات. فبالإضافة إلى بناء عناصر التهيئة، فإن هناك حاجة إلى وجود أدوات للاستعلام عن حالات تلك العناصر وتحسين أدائها.

- **أمن قاعدة بيانات إدارة التهيئة وأدوات وصول المستخدمين CMDB:** بينما يكون هناك حاجة دائمة لأمن تقنية المعلومات وأدوات لضبط عمليات الوصول إليها، فإن المسألة أصبحت أكثر أهمية فيما يخص قاعدة البيانات الشاملة والضخمة لإدارة التهيئة CMDB. تلك المنطقة التي يمكن لشخص ما فيها أن يحصل على صلاحيات وصول لجميع مصادر بيانات المؤسسة. لذا فوجود ضوابط أمنية قوية يعد من الأمور الأساسية في هذا المجال.

- **الأدوات الخاصة بإدارة تهيئة قاعدة البيانات:** تعد هذه إحدى الأدوات الخاصة بمجال قواعد البيانات التي يجب أن تكون متاحة لتصميم هياكل البيانات الخاصة بعناصر التهيئة، وذلك لتعزيز فاعلية قاعدة بيانات إدارة التهيئة CMDB. أما الأمر الأكثر أهمية، فهو أن هذا هو المجال الذي يجب أن تكون فيه أدوات الضبط القوية الخاصة بالمراجعة موضوعة في موضع التنفيذ.

- **إدارة البيانات ومستودع قاعدة البيانات:** يصف هذا العنصر قاعدة البيانات الفعلية، كما يصف برمجيات التشغيل لها وكذلك الضوابط المادية والبيئية الخاصة بها. لذا هناك حاجة لأخصائيين يتمتعون بمهارات عالية في مجال برمجيات قواعد البيانات لإدارة وضبط البرمجيات. وبالطبع لا بد من وجود عمليات صحيحة معمول بها فيما يخص النسخ الاحتياطي واستمرارية الأعمال.
- **ضوابط أمن وحماية البيانات:** كما أن هناك احتياجات لضوابط أمن ووصول قوية معمول بها على روابط واجهة المستخدم، فإن هذه العمليات الأمنية تكون أكثر أهمية لأنها تعمل مستودعات من قاعدة بيانات إدارة التهيئة (CMDB) وغيرها من نظم الاستخدام الأخرى.
- **مستودعات تكامل البيانات:** يجب أن يوفر التشغيل الكامل لقاعدة بيانات إدارة التهيئة CMDB وصلات إلى مجموعة عريضة من النظم والعمليات. ويعد هذا بمثابة رابط للنتائج الهامة بين قاعدة بيانات إدارة التهيئة CMDB والكيان الكبير للتطبيقات الأخرى.
- **الأدوات الخارجية للاكتشاف والمتابعة:** بالذهاب إلى ما هو أبعد من قاعدة البيانات الفعلية لإدارة التهيئة CMDB الخاصة بالمؤسسة، فإنه يجب أن يكون هناك مجموعة واسعة من الآخرين من الذين لديهم حاجة للوصول إلى بيانات CMDB ومراقبتها. فعلى سبيل المثال، قد يحتاج مدققو تقنية المعلومات إلى مراجعة هياكل بيانات محددة وعمليات أخرى ليست من ضمن عمليات المستخدمين الاعتيادية، ولا حتى من عمليات مسئول الرقابة.
- **مستودعات بيانات أخرى:** يبين الشكل التوضيحي (١٤-٣) أن قاعدة بيانات إدارة التهيئة CMDB هي بالعادة ليست المستودع المركزي الوحيد لبيانات التهيئة. بل سيكون هناك أدوات أخرى لقاعدة بيانات التهيئة كذلك. فبالنسبة لمستودع البيانات هذا أو أي مستودع آخر لقاعدة بيانات إدارة التهيئة CMDB، فإنه يجب أن يكون هناك ربط قائم ومعمول به مع تلك الواجهات الأخرى.

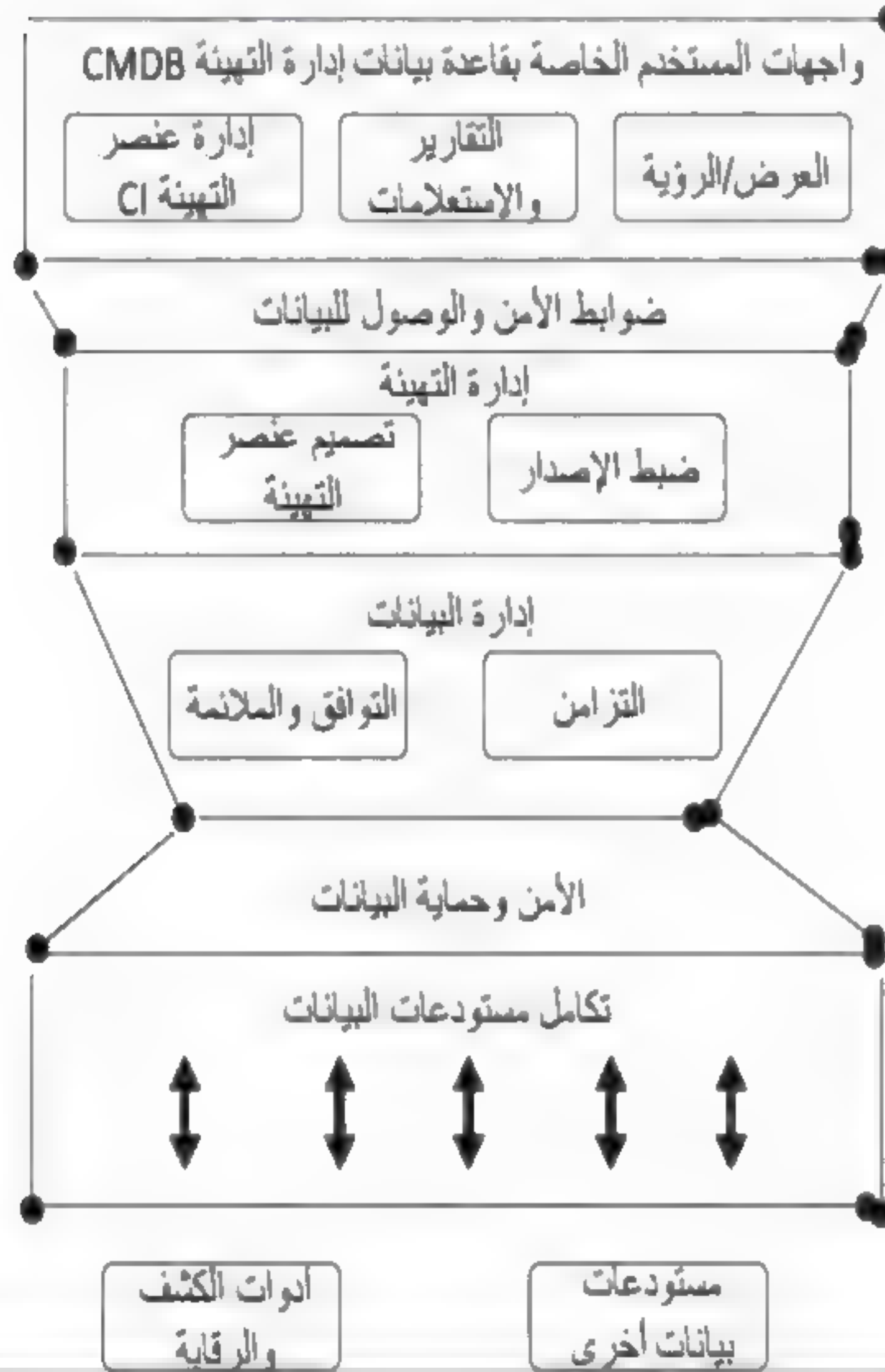
تصف القائمة السابقة خصائص قاعدة بيانات إدارة التهيئة CMDB. فبالنسبة للمؤسسات الكبيرة والمعقدة، سيكون من الصعب إطلاق وتنفيذ مثل هذه الإدارة والعملية الخاصة بتقنية المعلومات بشكل فعال، غير أنه يجب أن تكون هناك فوائد ومنافع مستمرة من قدرات وكفاءات النظم. إن تطبيق قاعدة بيانات فعالة لإدارة التهيئة CMDB يعد أحد الأدوات الهامة في كفاءة وحوكمة تقنية المعلومات بالنسبة لأي مؤسسة تمتلك مجموعة كبيرة ومعقدة نسبياً من نظم وعمليات تقنية المعلومات.

إنشاء قاعدة بيانات إدارة التهيئة CMDB في المؤسسة:

يعلن العديد من باعة البرمجيات عن منتجات خاصة بقاعدة بيانات إدارة التهيئة CMDB على أنها جزء من العروض الخاصة بهم. وبالرغم من أن معظم هذه المنتجات يجب أن تتفق ومعايير إطار العمل آيتل، إلا أنه لا يوجد تعريف موحد ومتناغم بين تلك المنتجات. وبينما يمكن لتطبيق قاعدة بيانات إدارة التهيئة CMDB أن يكون المشروع الرئيسي بالنسبة للمؤسسة، فإن إدارات تقنية المعلومات الأصغر والأقل نضجاً لا ترغب في الاستثمار في برامج قاعدة بيانات إدارة التهيئة CMDB المكلفة والمعقدة. حيث يمكنهم تنفيذ مجموعة محددة من عمليات إدارة التهيئة بواسطة استخدام أدوات برمجية مكتبية بسيطة مثل الإكسيل Excel. وتعد قاعدة بيانات إدارة التهيئة CMDB بمثابة نظام لإدارة المعرفة أكثر من كونها منتجاً من المنتجات البرمجية، كما أنها تعتبر فهرساً أكثر من كونها قاعدة بيانات معقدة. هذا يعني كلما كانت كمية البيانات الخاصة بعناصر التهيئة صغيرة استطاعت المؤسسة الاستفادة من مزايا قاعدة بيانات إدارة التهيئة CMDB من خلال عدة طرق - كالورق، أو مخططات VISIO، أو قواعد بيانات ACCESS، أو العقول البشرية، وما شابه. وهذا بالضبط ما تم تثبيته في العديد من المؤسسات.

شكل توضيحي (٣-١٤)

عرض تصوري لقاعدة بيانات إدارة التهيئة CMDB



من ناحية أخرى، فإنه عندما تتسع إدارة تقنية المعلومات في المؤسسة جغرافياً بشكل كبير، ويكون لديها مئات أو آلاف المستخدمين والمواقع، فإن هذا العدد الموهول لتلك الاختلافات في التهيئة يتطلب حلاً من نوع خاص لقاعدة بيانات إدارة التهيئة CMDB. إن تقنية المعلومات أو الفريق الإداري الذي يبحث عن الحل المناسب أو من يقوم بتثبيته يجب أن يقوم بوضع معايير ومتطلبات خاصة بأداء نظام قاعدة بيانات إدارة التهيئة

CMDB لديهم. لذا فإن نظام قاعدة بيانات إدارة التهيئة CMDB في المؤسسة يتطلب بعض المزايا الفريدة. وهي أولاً، إن الحل الحقيقي لقاعدة بيانات إدارة التهيئة CMDB يعتمد على مفهوم قديم في قاعدة البيانات يدعى نمذجة الأبعاد والذي فيه خروج بسيط عن النمط. وفيه يجب أن يكون الحل الخاص بقاعدة بيانات إدارة التهيئة في المؤسسة معتمداً على نموذج قاعدة بيانات الأبعاد بدلاً من قاعدة البيانات العلاقية الشائعة في الوقت الراهن. فقواعد البيانات العلاقية الموجودة هذه الأيام مثل أوراكل Oracle ودي بي تو DB2 الخاصة بشركة IBM لا تستطيع القيام بالمهمة المنوطة بقاعدة بيانات إدارة التهيئة CMDB.

وتعود هذه المفاهيم الخاصة بنماذج قواعد البيانات العلاقية المقابلة لنماذج قواعد بيانات الأبعاد إلى سبعينيات القرن الماضي مع العديد من القضايا المنسية من قبل معظمنا ممن عاصروها. في هذا القسم، سنقوم بشرح ما يحتاج إليه الحل البرمجي لقاعدة بيانات إدارة التهيئة CMDB على مستوى المؤسسة ومن هذه الاحتياجات: قاعدة بيانات الأبعاد واتحاد وتوافق وتزامن ونمذجة البيانات. وهنا لسنا بصدد تقديم مقالة تتحدث عن نمذجة قواعد البيانات، بل نهدف إلى إيجاز بعض المفاهيم الضرورية والرئيسية بالنسبة لقاعدة البيانات الفعالة لإدارة التهيئة CMDB.

معمارية قاعدة البيانات العلاقية مقابل معمارية قاعدة بيانات الأبعاد:

تستخدم قاعدة البيانات العلاقية أسلوب "الصف والعمود" الذي يشبه طريقة حفظ البيانات في الجداول الإلكترونية الخاصة ببرنامج الإكسل Excel أو في نظام معالجة المعاملات عبر الإنترنت. وسيكون من السهل هنا البحث عن البيانات المخزنة في قاعدة البيانات العلاقية في حال كنت تعرف مقدماً ما الذي تريد رؤيته. من ناحية أخرى، فإن قاعدة بيانات إدارة التهيئة CMDB لا تقوم بتخزين معظم بياناتها، فهي تشير إلى بيانات محفوظة في قواعد بيانات أخرى قد تكون علاقية. وتستخدم قاعدة بيانات إدارة التهيئة CMDB أيضاً لتقديم ما يطلق عليه التوعية السياقية على فئات من البيانات غير المترابطة بشكل واضح.

على سبيل المثال، قد يكون الاستعلام الشائع في قاعدة بيانات إدارة التهيئة CMDB هو "ما عدد المستخدمين في قسم المبيعات الذين استخدموا نظام SAP خلال الأسبوع الأخير

من الشهر؟". هذا النوع من الاستعلامات لا يتناسب بالمرّة مع قاعدة بيانات علاقية مركزية من خلال معاملات استعلام سبق بناؤها. حيث يوجد العديد فقط من التوليفات الممكنة بين البيانات. فهذا النوع من الاستعلامات يتعين عليه سحب البيانات من عدة نظم. ومن المحتمل ألا تكون البيانات التي يحتاج إليها هذا الاستعلام مصفوفة بشكل جيد في صفوف وأعمدة جاهزة للاستعلام. بل يجب على قاعدة بيانات إدارة التهيئة CMDB الخاصة بالمؤسسة أن تستخدم تقنية الأبعاد التي تمثل البيانات كما لو كانت أبعاداً أو مستويات مختلفة.

تشتمل أبعاد قاعدة بيانات إدارة التهيئة CMDB غالباً على الموقع (مثل المدينة والولاية والطابق ... إلخ) ومجموعات العمل مثل إدارة المبيعات وإدارة التسويق وما إلى ذلك، وكذلك خدمات تقنية المعلومات مثل ساب SAP أو البريد الإلكتروني والنطاقات الزمنية وغيرها. فبدلاً من استخدام جداول البيانات الإلكترونية الخاصة ببرنامج الإكسيل والمكونة من صفوف وأعمدة، ينبغي على المرء التفكير بأحد أنواع تمثيل البيانات الذي يدعى مكعب روبيك Rubik's Cube ليبدأ بتكوين الفكرة. فالمنطق المطلوب هنا ليس جديداً، فقد كان موجوداً معنا لسنوات لكن بشكل أطلقنا عليه مصطلح المعالجة التحليلية المباشرة المتصلة (Online Analytical Processing (OLAP. في جميع الأحوال، فإن التمثيل البسيط للمعالجة التحليلية المباشرة (المتصلة) OLAP لا يعطيك قاعدة بيانات إدارة التهيئة CMDB وذلك لسببين في غاية الخصوصية: أولهما، أن معظم البيانات الخاصة بقاعدة بيانات إدارة التهيئة CMDB توجد خارج نظام قاعدة البيانات نفسها. ولكي يتم سحب البيانات من مصادر متعددة فإن ذلك يتطلب اتحاداً federation - وهو تعبير طنانٌ جديدٌ في قاعدة بيانات إدارة التهيئة (CMDB). وهو ما سنتحدث عنه في الأقسام التالية.

اتحادية قاعدة البيانات Database Federation:

إن قاعدة بيانات إدارة التهيئة CMDB هي ما يطلق عليها قاعدة البيانات الوصفية Metadatabase. هذا يعني أنها عبارة عن قاعدة بيانات تشير إلى قواعد بيانات أخرى. فالشرط الرئيسي لقاعدة بيانات إدارة التهيئة هو ما يطلق عليه نموذج الأبعاد أو الاتحادية، وهي عبارة عن مراجع للبيانات من مصادر متعددة. وقد كانت القضية الخاصة بصحة

البيانات هي القضية التي أدت لأول مرة إلى اتحادية البيانات. فعندما تقوم بعمل نسخة من شيء ما، ما هو برأيك السند القطعي؟ الأصل أم النسخة؟ وكيف تستطيع أن تعرف أن النسخة هي الأصل نفسه؟

إن المفاهيم التي تدور حول اتحادية قاعدة بيانات إدارة التهيئة CMDB تتعلق بكيفية الاتصال بمصادر بيانات غير متجانسة والبت بشأن أي من أجزاء البيانات تكون مؤكدة ومن ثم إنشاء وحفظ مفاتيح لبيانات فريدة غير موجودة في أي من مصادر البيانات الخارجية إلا أنها لا تزال مطلوبة. على سبيل المثال، قد تكون البيانات غير الموجودة في أي نظام من هذه النظم هي اسم خدمة تقنية المعلومات ومن هم المستخدمون لها. كما يجب أن يكون هناك أيضاً طريقة لحفظ المعرفة (الوعي) Awareness بأنواع البيانات الموجودة في كل مصدر من مصادر البيانات التي تم توحيدها، وذلك لإجراء الاستعلامات الفورية أو المخصصة (غير المعرفة مسبقاً).

إن الفكرة الخاصة باتحادية قاعدة بيانات إدارة التهيئة CMDB تتطلب الاتصال بالعديد من مصادر البيانات، إلا أن امتلاك نظام قاعدة بيانات إدارة التهيئة سيسمح حقيقة بتوحيد تلك المصادر للبيانات. ويعد هذا أمراً في غاية الصعوبة على أرض الواقع. فالاتحاد هو واحد فقط من متطلبات الامتثال التقنية الأربعة لقاعدة بيانات إدارة التهيئة CMDB التي لها الدرجة نفسها من الصعوبة. لنأمل ذلك: ماذا لو كان هناك مخزان من البيانات يشيران إلى البيانات نفسها؟ أي مخزن بيانات يكون قطعي الدلالة؟ ثم، الأمر الأكثر أهمية، كيف تستطيع أنت أن تحدد أي منهما هو المؤكد؟ وتعد هذه من القضايا الخاصة بمطابقة وتوافقية البيانات.

توافقية البيانات في CMDB:

بصرف النظر عن قضية الاتصال بمصادر بيانات غير متجانسة، والتي من المحتمل أن تكون أيضاً تنافسية، يمكن أن تتم بكل بساطة، فالمشكلة الكبيرة التي تواجه عملية الاتحاد الخاصة بقاعدة بيانات إدارة التهيئة CMDB هي ما يسمى بمطابقة البيانات Data confrontation. أثناء إنشاء المعلومات السياقية لقاعدة البيانات الوصفية الخاصة بقاعدة بيانات إدارة التهيئة CMDB وصيانتها، يتم تحويل أجزاء أساسية من البيانات

من مصادر البيانات الموحدة إلى مخازن البيانات الخاصة بقاعدة بيانات إدارة التهيئة CMDB. ونظراً لأنه من الشائع أن يكون هناك عدة تطبيقات ونظم متداخلة تقوم بطلب الأصول الخاصة بتقنية المعلومات نفسها أو تحتفظ بالبيانات نفسها، فمن المحتمل أن يؤدي ذلك إلى عدم تناغم البيانات وتكرارها. وهذا هو ما يعرف بمطابقة البيانات.

توافقية البيانات Data reconciliation تعني تعديل أو تكييف البيانات المستمدة من أكثر من مصدر واحد لإنهاء التكرارات والحفاظ على تناغم البيانات. إذ لا فائدة من الاتحادية في ظل وجود مشكلة التوافقية. فالتوافقية على أية حال ليست نهاية المتطلبات بالنسبة لقاعدة بيانات إدارة التهيئة CMDB الخاصة بالمؤسسة، فما يضيف مزيداً من التعقيد لنظام قاعدة بيانات إدارة البنية CMDB هو الحاجة إلى معالجة أي تغيرات ناجمة من التسويات الصحيحة والناجمة للبيانات، وهذا ما يقودنا إلى ما يعرف بالتزامن Synchronization.

تزامن بيانات CMDB:

يمكن أن تتغير البيانات المخزنة في قاعدة بيانات إدارة التهيئة CMDB الموحدة عند وقوع أحداث كتغيير اسم مدير المشروع (مثال "المستخدم") أو تغيير نوع المعدات المستخدمة من Cisco series 2504 software مثلاً إلى Cisco 2801. لذا يجب أن تكون عملية توافقية البيانات قادرة على حل هذه الاختلافات للمحافظة على سلامة بيانات قاعدة بيانات إدارة التهيئة CMDB. لكن هذه تقنية معلومات وليست مستودع بيانات "بسيطاً". فلا ينبغي تغيير أي عنصر من عناصر التهيئة CI الموجودة في قاعدة بيانات إدارة التهيئة التي تتفق مع آيتل دون أن يكون هناك طلب للتغيير. ومن ثم فإن نظام قاعدة بيانات إدارة التهيئة CMDB الذي يستطيع أن يوحد ويعمل على توفيق البيانات بنجاح يجب عليه أيضاً أن يكون قادراً على التنبيه عندما يتم الكشف عن تغيرات غير مصرح بها وغير مخطط لها. فالإخفاق في مزامنة التغيرات التي تمت تسويتها سرعان ما يؤدي إلى الخروج عن سيطرة قاعدة بيانات إدارة التهيئة CMDB، وهو ما يمكن وصفه بالكارثة.

هذا يعني أن نظام قاعدة بيانات إدارة التهيئة CMDB بحاجة إلى معرفة التغيرات التي تمت الموافقة عليها. ثم عندما يقوم محرك توافقية البيانات بكشف وتحليل لأحد

التغيرات في البنية التحتية أو في البيانات، فعليه أن يقوم بمقارنة هذا التغيير بقائمة التغيرات المعتمدة المتوقعة وأن يقوم بإصدار تنبيه في حال كان التغيير غير معتمد أن (يكون غير مخطط له مثلاً). هذا التنبيه يلفت انتباه مديري قاعدة بيانات إدارة التهيئة CMDB للبيانات الخاصة بقاعدة البيانات هذه. هؤلاء المديرون بحاجة إلى مساعدة بيانات معروضة وتصويرية ورسومية. وهو المتطلب التقني الرئيسي التالي للنمذجة.

نمذجة CMDB:

النمذجة Modeling هي مناظرة العلاقات المركبة في قاعدة البيانات ووضع تصور لها. وهي عبارة عن تعريفات لخدمات تقنية المعلومات وروابط بين عناصر التهيئة CIs. فالنمذجة هي أكثر من مجرد تقرير أو عرض قوائم للموارد على شكل أشجار وفروع. لذا يتعين على قاعدة بيانات إدارة التهيئة CMDB أن تكون قادرة على عرض بياناتها بصورة واضحة وبطرق تسمح للناس باستخدام تلك المعلومات لتقييم الآثار المترتبة على إدارة التغيير، وتحديد صلاحيات إدارة مكتب الدعم الخاص بإدارة تقنية المعلومات، واكتشاف الأعطال وإصلاحها من خلال العمليات الخاصة بإدارة الحوادث والمشاكل، والعشرات من الاستعلامات الفورية Ad hoc queries من جميع العمليات التشغيلية الخاصة بتقنية المعلومات.

إن مطلب النمذجة هذا يذهب إلى ما هو أبعد من مجرد قوائم بسيطة "لشجرة أدلة" كالتى نجدها بشكل شائع في بعض منتجات قاعدة بيانات إدارة التهيئة CMDB. فلا قيمة لكل من اتحاد وتوافقية وتزامن البيانات في حال لم يتمكن المستخدمون من الحصول على إجابات نهائية ومفهومة على أسئلتهم المعقدة في أسرع وقت ممكن. ويتطلب هذا في أغلب الأحيان تمثيل العلاقات المعقدة بين عناصر البنية CIs بشكل بياني حسب الطلب. باختصار، إن قاعدة بيانات إدارة التهيئة CMDB في المؤسسة ليست وحيدة، إنما هي عبارة عن نظام معقد يتعين عليه توحيد مخازن أخرى للبيانات، والتوفيق بين المنظورات البديلة أو المختلفة للبيانات نفسها، والكشف عن التغيرات غير المصرح بها، والعمل على مزامنة التغيرات المعتمدة مع مخازن البيانات الوصفية الخاصة بها وأن يكون قادر على تمثيل الهياكل (التكوينات) بيانياً وبشكل متغير حسب الطلب. وهذا ليس بالأمر السهل.

يجب على المؤسسة التي تقوم بتطوير قاعدة بيانات إدارة التهيئة CMDB الخاصة بها أن تتعهد تلك المفاهيم المتعلقة بالنمذجة المتعددة الأبعاد، وقضايا الاتحاد، والتوافقية والتزامن والنمذجة بشكل شمولي. وبالرغم من أن المدير الأول الذي يقوم بتقييم الخطط الخاصة بقاعدة بيانات إدارة التهيئة CMDB أو النظم المثبتة قد لا يكون لديه مستوى معين من الإلمام بهذه المفاهيم الخاصة بعلوم الحاسب؛ فإنه من المناسب جداً بالنسبة للمدير الأول أن يسأل أحد العاملين لديه في إدارة تقنية المعلومات عن كيفية التعامل مع هذه المسائل. وفي حال عدم ارتياحه لتلك الإجابات، فربما من الضروري العمل مع استشاري في تلك القضايا.

في جميع الأحوال، ينبغي على المؤسسة التي تعمل على إطلاق قاعدة بيانات إدارة التهيئة CMDB أن تقوم بوضع عمليات مراقبة وضمان حدوث الاتحاد، والتوافق، والتزامن والنمذجة. فالإخفاق في إدارة تلك القضايا الحساسة والحرجة يمكن أن يحول وبشكل سريع مشروع قاعدة بيانات إدارة التهيئة CMDB من أصل Asset إلى التزم Liability.

إدارة محفظة تقنية المعلومات:

من الطبيعي أن يكون كل من إدارة تقنية المعلومات ومستخدمي تلك النظم والعمليات قد قاموا مع مرور الوقت بتنفيذ أعداد كبيرة من النظم والعمليات المرتبطة بنظم أخرى، سواء كان بشكل مباشر أم غير مباشر، أو أن تكون نظاماً مستقلة وقائمة بذاتها. وفي العادة قد تم تعيين مديري تقنية المعلومات مسئولين عن بعض تلك النظم والعمليات. في حين أن الإدارات الخاصة بمستخدمي تقنية المعلومات قد يضطلعون بالمسؤولية المباشرة عن النظم والعمليات الأخرى. إلا أن كل مدير مسؤول يعتقد غالباً أن النظم الخاصة به أو بها هي الأكثر أهمية عندما يكون هناك خلافات في إعداد الجداول الزمنية للأعمال أو وجود حاجة خاصة لإجراء تعديلات، أو احتياجات أخرى متعلقة بالنظم. وتتمكن إدارة تقنية المعلومات عادة من تحقيق بعض الفوائض المالية الكبيرة الخاصة بالخدمات والاستثمارات، وذلك إذا نظرت إلى تلك النظم والعمليات الخاصة بتقنية المعلومات والتي تكون غالباً متفاوتة وتقوم بإدارتها على أنها محافظ لموارد تقنية المعلومات portfolios of IT resources.

إن إدارة محفظة تقنية المعلومات تعني تقسيم وإعادة تصنيف وتطبيق إدارة الأصناف الكبيرة من موارد تقنية المعلومات. فمبادرات نظم التخطيط والمشاريع الرئيسية والجديدة في تقنية المعلومات والخدمات المستمرة لدعم تطبيقات تقنية المعلومات يمكن اعتبارها أمثلة على محافظ تقنية المعلومات.

إن الالتزام الخاص بإدارة محفظة تقنية المعلومات هو تحديد مقدار الجهود غير الرسمية لتقنية المعلومات مقدماً وتفعيل القياسات والتقييمات الموضوعية للتصورات الخاصة بالاستثمار. فمفهوم إدارة محفظة تقنية المعلومات مشابه لإدارة المحفظة المالية إلا أن هناك اختلافات كبيرة بينهما. إذ تكون أصول المحفظة المالية في العادة عبارة عن معايير ثابتة لمعلومات قياسية مثل عوائد الاستثمار. من ناحية أخرى، فإن عملية قياس قيمة تقنية المعلومات تحتاج غالباً إلى جهود كبيرة. المشكلة هي أن استثمارات تقنية المعلومات ليست متاحة كما هو الحال بالنسبة للأسهم والسندات المالية يتم غالباً قياس قيمتها باستخدام مقاييس غير مالية. هذا بالإضافة إلى أن أصول محفظة تقنية المعلومات لديها علاقة وظيفية مع المنظمة. مثل نظام إدارة المخزون الخاص بالإمدادات أو نظام الموارد البشرية الخاص بمتابعة أوضاع الموظفين. ونظراً لأهميتهم بالنسبة للمؤسسة، فمن الصعب قياسهم باعتبارها أحد أشكال محافظ تقنية المعلومات.

تقدم إدارة محفظة تقنية المعلومات مزايا وفوائد تفوق الأساليب والطرق المتبعة في الاستثمارات الخاصة بتقنية المعلومات. كما أن هناك مزايا أخرى تشمل الرقابة المركزية على الميزانية، وإدارة المخاطر، والتوافق الإستراتيجي لاستثمارات تقنية المعلومات، وطلبات استخدام النظم، وإدارة الاستثمارات إلى جانب توحيد إجراءات وقواعد وخطط الاستثمارات.

تطبيق إدارة محفظة تقنية المعلومات:

يجب على إدارة تقنية المعلومات وبالاتفاق مع المستخدمين الرئيسيين الآخرين للنظم أن يقوموا بوضع نهج إدارة المحافظ لإدارة موارد تقنية المعلومات الخاصة بها وتطوير الأهداف العامة وغايات الأداء المرجوة منها. وتختلف إدارة المحفظة عن الإدارة المالية

لتقنية المعلومات في أن لها توجهاً صريحاً وهو أن الهدف الإستراتيجي لها يرمي إلى تحديد الاستثمارات التي يجب أن نستمر فيها والاستثمارات التي يجب الانسحاب منها.

يتم تطبيق إدارة محفظة تقنية المعلومات بالنسبة للعديد من المؤسسات من خلال تقسيم موارد النظم الخاصة بها إلى ثلاثة مجالات واسعة للمحفظة مع محافظ جزئية بداخل كل مجموعة:

١- محافظ التطبيقات: يمكن أن تحتوي هذه المحافظ على جميع التطبيقات الإنتاجية. ويمكن أيضاً تقسيمها إلى محافظ جزئية لمجموعات مختلفة من التطبيقات مثل المالية والتطبيقات الإنتاجية الخاصة بالتصنيع وتطوير المنتجات الهندسية. الفكرة هنا هي العمل على تطابق وإدارة المحافظ التي لها المفاهيم والأهداف نفسها، كأن تكون هناك محفظة مخصصة للتطبيقات المتعلقة بالرواتب ونظم الموارد البشرية وتطبيقات تدريب الموظفين.

ويجب أن تستند محافظ التطبيقات إلى النظم القائمة مثل النظم المعتمدة على المقرر الرئيسي للمؤسسة، ونظم الوحدات الميدانية والدولية والنظم الخاضعة لسيطرة المستخدم النهائي. كما يجب أن تستند جميع هذه المحافظ إلى قيمتها النسبية في المؤسسة. ويمكن أيضاً أن تستند المقارنات والتقييمات إلى مستوى المساهمة في الربحية التي تعود من استثمارات تقنية المعلومات. هذا بالإضافة إلى أنه قد تستند هذه المقارنة إلى عوامل غير ملموسة كمستوى خبرة إدارة تقنية المعلومات في تقنية محددة أو مدى إلمام مستخدميها بالتطبيقات والبنية التحتية أو قوى خارجية كظهور تقنيات جديدة وزوال أخرى قديمة.

٢- محافظ البنية التحتية: تركز هذه الأنواع من المحافظ على تقنية المعلومات والعمليات البرمجية الخاصة بإدارة البنية التحتية. ففي بعض الأحيان يتم تقسيم إدارة البنية التحتية إلى فئات من إدارة النظم، وإدارة الشبكة، والأمن، وبرامج إدارة التخزين. إن قدرة المؤسسات على استغلال البنية التحتية والعمليات التشغيلية وإدارة حلول التوريد والخدمات الخاصة بتقنية المعلومات لا يتوقف على إتاحة وتكلفة وفاعلية التطبيقات والخدمات فحسب، وإنما يساعد إدارة تقنية المعلومات أيضاً على الوصول إلى اتفاقات مع مقدمي الخدمات من أجل إدارة كامل عملية التوريد. وسعياً منهم

لتقليل التكاليف، وزيادة جودة تقنية المعلومات، وزيادة القدرة التنافسية للمؤسسات من خلال انتقاء مصادر وخدمات تقنية المعلومات. فإن العديد من المؤسسات وإدارات تقنية المعلومات التابعة لها لا ينظرون إلى الجانب الإداري من المعادلة. ومن النتائج التي يمكن التنبؤ بها جراء هذا الإهمال هي المدفوعات الزائدة، وتجاوزات التكاليف، وتوقعات لم تتحقق، والفشل التام.

تساعد عملية إدارة محافظ نظم برمجيات البنية التحتية لتقنية المعلومات المختصين بالبرمجيات على اتخاذ بعض القرارات الصعبة. على سبيل المثال، هل نحن بالفعل نريد الترقية إلى إصدار جديد لإحدى قواعد البيانات لدينا؟ في حال كانت الإجابة نعم، كيف سيتفاعل تطبيق قاعدة البيانات هذا مع عمليات قواعد البيانات المماثلة في جميع أنحاء المؤسسة؟ ما التكلفة الكلية التي ستحملها المؤسسة جراء استخدام هذا المنتج؟ وما القيم التي ستحصل عليها المؤسسة منه؟

٣- محافظ المشاريع: ينبغي على إدارة المحافظ معالجة قضايا الإنفاق على تطوير القدرات الابتكارية من حيث العائد المحتمل من الاستثمار (ROI) أو return on investment أو الحد من تدخل الاستثمارات في حالات حدوث إعادة تنظيم، أو استحواذ، أو الامتثال للوائح القانونية والتنظيمية. ويمكن الحكم على القضايا الإدارية مع إدارة محفظة المشاريع من خلال معايير مثل عائد الاستثمار ROI والتوافق الإستراتيجي ونظافة البيانات وفوائض الصيانة وملاءمة الحل الناتج والقيمة النسبية للاستثمارات الجديدة لاستبدال هذه المشاريع.

مارست العديد من المؤسسات نشاط إدارة المحافظ على مختلف مشاريع تقنية المعلومات والمشاريع التشغيلية لديها من خلال تأسيس مكاتب لإدارة المشاريع. وسيتم مناقشة عمليات إدارة المشاريع والبرامج في الفصل السادس عشر من هذا الكتاب.

مقاييس المحفظة: تحقيق القيمة من خلال إدارة محفظة تقنية المعلومات:

لن يكون لعملية تقسيم تطبيقات تقنية المعلومات والمصادر الأخرى إلى محافظ منفصلة قيمة كبيرة بالنسبة للمؤسسة ما لم يتم وضع بعض المقاييس لتقييم قيم المحافظ

والمساعدة في اتخاذ قرارات أخرى متعلقة بمحافظ تقنية المعلومات. يجب أن نتذكر أن محفظة تقنية المعلومات هي عبارة عن مجموعة من المبادرات والمشاريع و/ أو البرامج التي تحقق فوائد وتأثيرات واسعة المدى.

وعلى الرغم من أن لدينا مجموعة متنوعة من محافظ تقنية المعلومات التي تم إنشاؤها، فإنه ينبغي على المجموعات الإدارية المناسبة وضع مهمة سارية لكل محفظة من هذه المحافظ المتنوعة لتقنية المعلومات. قد يكون للمرء هدف نحو تعزيز نمو الأعمال في مجالات محددة تمت تغطيتها بواسطة مجموعة من التطبيقات بواسطة عدة مليارات من الدولارات، في حين قد يسعى شخص آخر إلى تحقيق زيادة ملحوظة في مستوى رضا العميل، وآخر قد يسعى إلى زيادة إيرادات المؤسسة من خلال تطوير منتجات جديدة.

الخطوة التالية هي بناء إستراتيجيات لتحقيق كل هدف من أهداف المحافظ ومن ثم وضع مقاييس لقياس مدى نجاحها. وتتقضي النظرة الشمولية هنا أن ننظر إلى مختلف تطبيقات وموارد تقنية المعلومات من حيث حجم مساهمتها في تحقيق القيمة المكتسبة من جميع العمليات التشغيلية الخاصة بالمؤسسة. وبالطبع عندما تفشل المحفظة في تحقيق رسالتها وأهدافها المرجوة، فقد يكون هذا هو الوقت المناسب لإجراء بعض التغييرات وربما يشتمل هذا على إعادة تشكيل مكونات المحفظة، أو تغيير الأساليب بشكل كامل أو جلب أشخاص آخرين والزج بهم في هذا الخليط.

يتعين على عمليات إدارة محفظة تقنية المعلومات وكذلك النظم القوية لإدارة التهيئة، أن تحسّن الأداء الشامل لتقنية المعلومات وتحسّن كذلك العمليات التشغيلية لحوكمة تقنية المعلومات. كما يجب على كل من هذين المجالين تشجيع كل من موظفي تقنية المعلومات والإدارة العامة على التفكير بشكل أفضل بالعمليات التشغيلية لتقنية المعلومات كما لو كانت مشاريع استثمارية لأعمال المؤسسة.

EV.

الفصل الخامس عشر

عمليات تنفيذ النظم التطبيقية وحوكمة تقنية المعلومات

كانت عملية تطوير النظم التطبيقية في فترة من الفترات مصدر قلق كبير بالنسبة لإدارات تقنية المعلومات. وذلك عندما كانت معظم وحدات برمجة وتطوير نظم تقنية المعلومات تقوم بتصميم النظم الجديدة الخاصة بها وتكتب البرامج باستخدام موارد قسم تقنية المعلومات وتقوم بتنفيذ واختبار المكونات البرمجية الأساسية للتطبيقات الجديدة. وقد كانت عملية التطوير هذه في بعض الأحيان تقود بعض المؤسسات إلى نفق مظلم. وكان يتم عادة تسليم تطبيقات تقنية المعلومات الجديدة المحلية أو المطورة داخلياً في وقت متأخر أي بعد الوقت المحدد بكثير، وكان يتم اختبار تلك الأنظمة بشكل ضعيف، ولم تكن تحقق أهدافها المعلنة. والأسوأ من ذلك، أنه كان في بعض الأحيان يتم إطلاق مشاريع تطبيقات جديدة دون فهم واضح لأهداف النظام. ويعود هذا العصر من مشاريع تطوير التطبيقات الفاشلة إلى الأيام الأولى لظهور تقنية المعلومات. وذلك عندما شعر الجميع بأن متطلبات نظم تقنية المعلومات الخاصة بهم عبارة عن متطلبات فريدة من نوعها وخاصة بأنظمتهم فقط. الأمر الذي استوجب عليهم القيام بتطوير التطبيقات الخاصة بهم لدعم وتحقيق تلك المتطلبات الفريدة والخاصة بهم.

وفي الوقت الذي كان مؤلف هذا الكتاب يسترجع تاريخه ليبين ذلك، فقد أقر بأنه كان يعمل ذات يوم في إحدى شركات تقنية المعلومات حيث كانت هناك جهود خاصة بتطوير النظم من أجل تطوير تطبيقات جديدة خاصة بحسابات المدفوعات - وقد كان آنذاك عبارة عن تطبيق لتحرير الشيكات بصورة فعالة - أو حتى لتطوير وبرمجة نظم جديدة لمعالجة الرواتب! وذلك في ضوء القوانين الخاصة بالولاية أو القوانين الوطنية، فقد كان هناك بالفعل اختلافات ضئيلة بين المتطلبات الخاصة بأحد نظم الرواتب مقابل متطلبات غيره من النظم. من جهة أخرى، وبالعودة إلى تلك الأيام فقد كان هناك عدد قليل من التطبيقات التي يتم تطويرها بشكل تجاري لاستئجارها أو شرائها. أما اليوم، فإننا بشكل عام نقوم بشراء هذا النوع من البرمجيات من أحد الموردين الخارجيين الذين يقومون

بتوريد البرمجيات والتحديثات الخاصة بها على نظام حاسبات الخادم - العميل الموجود في مكاتب المؤسسة أو إتاحة تلك البرمجيات من خلال بيئة الحوسبة السحابية (انظر الفصل التاسع من هذا الكتاب الذي يتحدث عن الحوسبة السحابية).

وعلى الرغم من الانتقال هذه الأيام من التطبيقات المطورة داخلياً إلى التركيز أكثر على البرمجيات التي يتم شراؤها وتوريدها من قبل أحد الباعة؛ لا تزال هناك حاجة لدى المؤسسة بأن تقوم بتطوير وبناء واختبار بعض نظم التطبيقات الخاصة بها أو أن تقوم بالتعديل على بعض التطبيقات التي قامت بشرائها. ويعد هذا الأمر واقعياً على وجه الخصوص عندما تقوم المؤسسة بتطبيق أحد نظم قواعد البيانات المعقدة ذات المهام المتعددة والمتراطة والمعروفة بنظم تخطيط موارد المؤسسة أي **Enterprise Resource Planning (ERP)**. حيث تمتلك هذه النظم المعقدة التي يتم توفيرها من قبل الباعة القدرة على ربط جميع وظائف التطبيقات تقريباً في مجموعة واحدة من قواعد البيانات المترابطة. على سبيل المثال، عند تثبيت نظام ERP في بيئة نظام صناعي، فإن تنفيذ طلب شراء منتج قد يتسبب في إحداث تغيرات في كل من نظام التصنيع ونظام الإنتاج، حيث يتم وضع أمر التوريد عند الحاجة إلى مواد إضافية وغيرها من العمليات الكاملة لبيع وشحن الانتاج.

وكعنصر أساسي من عناصر العمليات الرشيدة لحوكمة تقنية المعلومات، فإن المؤسسة تحتاج إلى عمليات قوية لتطوير نظم تقنية المعلومات، سواء لبناء تطبيقات بطرق تقليدية أم للحصول على ترخيص من البائع فيما يخص التطبيق السحابي.

يناقش هذا الفصل الجوانب الخاصة بحوكمة تقنية المعلومات فيما يتعلق بأساليب تطوير التطبيقات الخاصة بتقنية المعلومات من منظور التطبيقات التي تم تطويرها عبر عمليات تطوير نظم معتمدة ومعروفة جيداً، مروراً بالعمليات الشائعة لتطوير التطبيقات السريعة باستخدام تطبيقات لإنشاء أنواع مختلفة من التقارير، ووصولاً إلى قواعد البيانات الشاملة لنظام تخطيط موارد المؤسسة ERP. لذا يجب أن يكون لدى إدارة المؤسسة فهم جيد لعمليات حوكمة تقنية المعلومات التي تحيط بجهودها المبذولة لتطوير تطبيقات نظم جديدة.

دورة حياة تطوير النظم: إحدى التقنيات الأساسية لتطوير التطبيقات:

لقد كانت السنوات الأولى لتطوير تطبيقات تقنية المعلومات مليئة بالكوارث فيما يخص النظم الجديدة في العديد من المؤسسات. كان المدير الأول - غالباً المراقب المالي للمنظمة - يقوم بإخبار رئيس قسم تقنية المعلومات بأنه يريد تطبيقاً جديداً لتحقيق حاجة ما. وبدون إجراء المزيد من عمليات التحليل يقوم فريق البرمجة بالتجمع لكتابة برامج لتلبية هذه الحاجة. وكانت النتائج فاشلة غالباً. حتى وإن كانت تلك التطبيقات الجديدة تعمل وتم تسليمها في الموعد المناسب، فإنها لم تكن تلبى غالباً متطلبات وتوقعات الإدارة. إننا نتكلم هنا عن الأيام الأولى لنظم الحاسبات المركزية mainframe لتقنية المعلومات عندما كانت عملية شراء البرمجيات غير معروفة وكان الجميع يقومون بإنتاج التطبيقات الخاصة بهم.

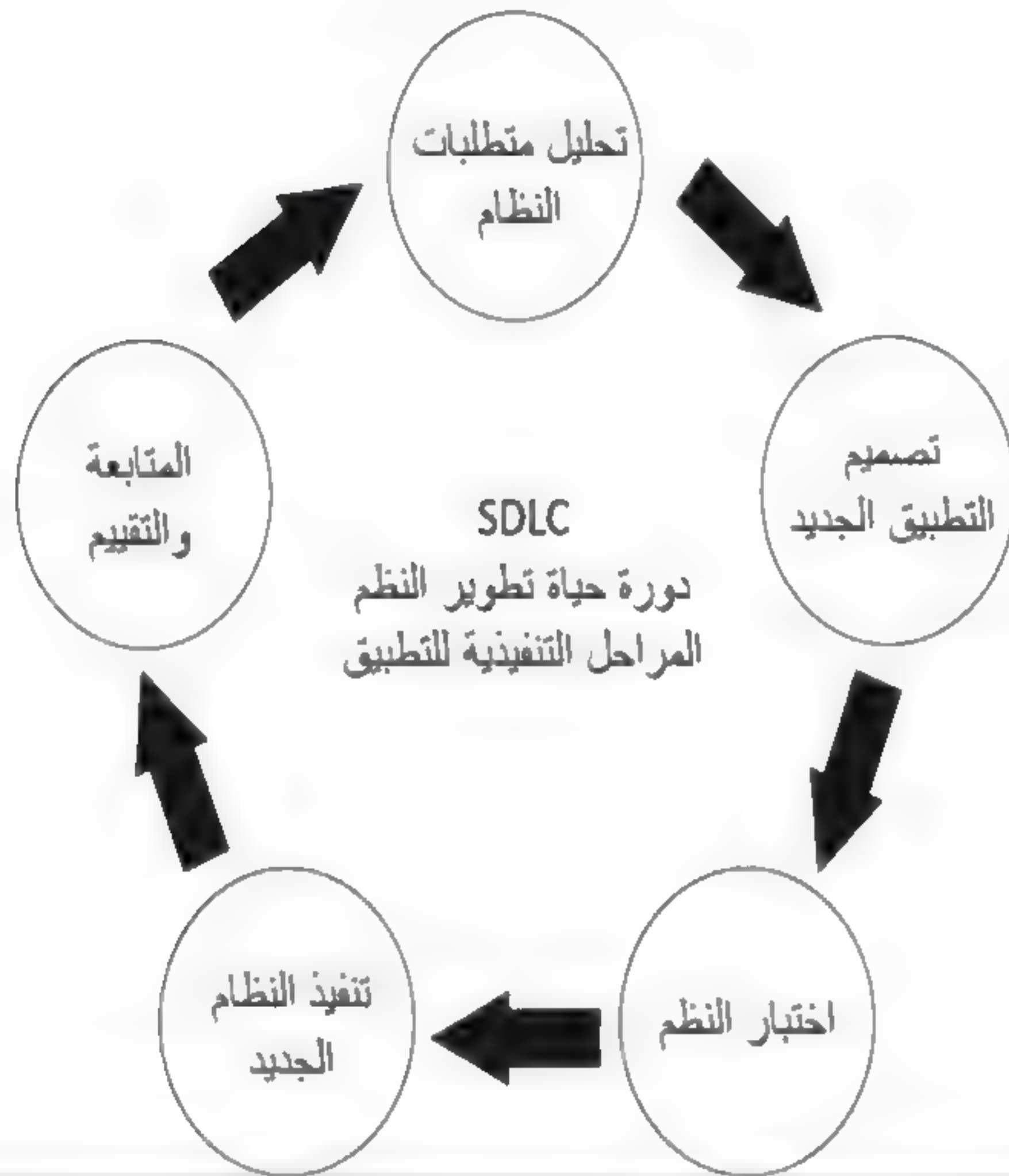
بالتأكيد لم تكن المفاهيم الخاصة بحوكمة تقنية المعلومات معروفة في تلك الأيام المبكرة التي كانت تتميز بوجود نظم الحاسبات المركزية، وبرامج الكوبول COBOL، والتي كانت تتميز بوجه خاص بوجود النظم الموجهة نحو الدفعة batch-oriented systems، وقد كان هناك بالتأكيد العديد من الإخفاقات الخاصة بتطوير التطبيقات. ولتنظيم عملية تطوير النظم وقتها، قامت شركة IBM وهي المزود الرئيسي للمعدات والبرمجيات في تلك الأيام بإطلاق نهج خاص بتطوير النظم عُرف بدورة حياة تطوير النظم Systems Development Life Cycle (SDLC). وعلى الرغم من محاولة العديد من الشركات الأخرى إنتاج أساليب أخرى مختلفة لتطوير النظم، فإن نهج SDLC أصبح بمثابة العملية الرئيسية لتطوير التطبيقات الفعالة في تقنية المعلومات.

يعرض الشكل التوضيحي (١٥-١) الخطوات العملية الأساسية لنهج SDLC في شكل عملية دائرية أو مستمرة. ومع أن المؤسسة وإدارة تقنية المعلومات التابعة لها بإمكانهم البدء بعملية تطوير النظم من أي نقطة، فإن هناك أولاً حاجة لعملية تحليل المتطلبات، وهذا يعني أنه قبل أن تبدأ وحدة تقنية المعلومات بأي عمل يتعلق بتطوير النظم، يجب عليها أولاً الحصول على تفاهم رسمي حول الأهداف والتوقعات الخاصة بمشروع النظام الجديد. ومن الطبيعي أن يتم التوثيق والتصديق على ما تم الاتفاق عليه من خلال عملية إدارية مع عمل تقديرات أولية لتكاليف النظام الجديد والفوائد المتوقعة منه.

وبمجرد أن تتم الموافقة على التطبيق الجديد، يتعين الانتقال إلى مرحلة أخرى رسمية من تصميم وبرمجة التطبيق. ويجب أن يتم تطوير وتوثيق كل برنامج ومكون من برامج ومكونات النظام الجديد ومن ثم اختباره باعتباره وحدة مستقلة. ثم ننتقل بعدها إلى مرحلة اختبار وتطبيق النظم بالكامل، الأمر الذي يؤدي إلى تطبيق النظام.

شكل توضيحي (١٥-١)

مراحل دورة حياة تطوير النظم SDL



إن المفهوم الشامل من وراء عملية دورة حياة تطوير النظم SDLC هي أنه عند تنفيذ تطبيق جديد، ينبغي على إدارة تقنية المعلومات وإدارة المؤسسة مراقبة نجاح وتقدم هذا التطبيق الجديد. الأمر الذي قد يؤدي إلى الحاجة إلى إجراء تعديلات أو تنقيحات على النظام أو الحاجة إلى نظام جديد كلياً. ومن ثم فإن دورة حياة تطوير النظم SDLC هي عملية تحسين مستمرة تهدف إلى تطوير التطبيقات الجديدة الخاصة بتقنية المعلومات ومراقبتها بشكل مستمر. وتعود عملية دورة حياة تطوير النظم SDLC تاريخياً إلى زمن نظم الحواسيب المركزية ونظم الدفعة التي كانت وقتها تحتاج إلى موافقات ووثائق تفصيلية كثيرة لكل خطوة من خطوات العملية.

وعلى الرغم من تحولنا الآن إلى التطوير السريع وعمليات تطوير تطبيقات النماذج التي تعتمد بشكل كبير على البرمجيات التي يوفرها البائع، فإن العناصر الرئيسية لعملية دورة حياة تطوير النظم SDLC يجب أن تبقى في موضع التنفيذ بالنسبة لأي عملية تطوير لتطبيقات جديدة في تقنية المعلومات. هذا يعني أن تطبيقات النظم الجديدة يجب أن تسير دائماً من خلال عملية رسمية لتحليل متطلبات النظم وعمليات رسمية لإطلاق التطبيقات وعمليات لتحسين تلك التطبيقات والاستغناء عنها في أواخر حياتها.

بالاعتماد على نوع وطبيعة عملية تطوير نظم تطبيقات تقنية المعلومات، فإن عملية تحليل المتطلبات يمكن أن تكون غير رسمية أو رسمية للغاية. إلا أن الشكل التوضيحي (١٥-٢) يوجز لنا محتويات العملية التقليدية لتحليل متطلبات تطوير النظم. إن المفتاح الرئيسي لهذه العملية هو أنه يجب على فريق المشروع أن يلقي نظرة فاحصة على طلبات المستخدمين وحتى على طلبات إدارة تقنية المعلومات المتعلقة بالتطبيق الجديد وتحديد ما إذا كانت هذه الطلبات منطقية أم لا. ما يحدث في الواقع، هو أن العديد من الطلبات الخاصة بتطبيق تقنية المعلومات يتم استبعادها بعد التحليل الأولي للنظم. وعلى أي حال، فإن عملية تحليل المتطلبات توفر آلية رسمية لمراجعة الطلبات الجديدة الخاصة بالتطبيق الجديد وتحديد ما إذا كانت هذه الطلبات منطقية أم لا.

يعد تحليل المتطلبات خطوة واحدة فقط من الخطوات الموجودة في دورة حياة تطوير النظم، إلا أنه يجب تضمينها دائماً في عملية تطوير النظم. وكأحد المكونات الرئيسية في عملية

حوكمة تقنية المعلومات، فإنه ينبغي على المؤسسة وإدارة تقنية المعلومات التابعة لها أن تمتلك نموذجاً من النماذج المعمول بها لعملية دورة حياة تطوير النظم SDLC، حتى في حال استخدامهم لعمليات التطوير السريع، كالنمذجة التي سنتحدث عنها في الفقرات التالية.

عمليات التطوير السريع في تقنية المعلومات: النمذجة (Prototyping):

إن استخدام العمليات الرسمية لدورة حياة تطوير النظم SDLC كان له أثر ومعنى كبير في الأيام الأولى لنظم تقنية المعلومات، وذلك عندما كانت المؤسسات هي التي تقوم بتطوير وبرمجة تطبيقاتها بشكل كامل، وعندما كان هناك حاجة لتوثيق وصياغة عمليات تطوير النظم الجديدة بشكل رسمي. وقد كان، هناك مجموعة متنوعة من التجار الذين قاموا ببيع أساليب تطوير الأعمال وإدارات تقنية المعلومات التابعة لها. وقد كانت المنتجات التي يتم تسويقها في ذلك الوقت تطلب من مطوري النظم أن يقوموا بتحضير وثائق تفصيلية عن جميع مراحل الأعمال التي قاموا بإنجازها. وباتباع ذلك بالشكل السليم، أدت تلك المنهجيات إلى الوصول لنظم تطبيقات جديدة موثقة ومخطط لها على نحو جيد. كان هدفها هو مجرد تحسين عملية تطوير وتنفيذ التطبيقات الجديدة لتقنية المعلومات. وقد كانت المشكلة الوحيدة وقتها أن المنهجيات الكثيرة الخاصة بتطوير الوثائق كانت في كثير من الأحيان لا تعمل بشكل جيد. فقد كانت المنهجيات المنشورة وقتها تتطلب استكمال العديد من الوثائق الرسمية، وجميعها يحتاج إلى مراجعات وموافقات. ومع ذلك، فقد قامت كل من وحدة تقنية المعلومات والإدارة بالنظر في أعمال التطوير الجديدة وكانت باستمرار تقرر أموراً ليست صحيحة تماماً وتبحث باستمرار عن تغيرات وتنقيحات تكون ثانوية غالباً.

لم يعد هناك وجود بالأساس لبائعي هذه المنهجيات الرسمية المنشورة لدورة حياة تطوير النظم SDLC، تماماً كما ابتعدنا نحن عن النظم الرسمية للحاسبات المركزية Mainframe. أما اليوم فهناك تطبيقات جديدة يتم بناؤها غالباً من خلال أدوات برمجية سهلة الاستخدام تعتمد على الجداول. حيث إننا نقوم ببناء إصدار أولي أو نموذجي، ومن ثم نقوم بتعديل هذا النموذج ليتوافق مع المتطلبات، ثم نقوم بتنفيذ التطبيق. هذه الأنواع من التطبيقات تم تطويرها من خلال عملية تسمى التطوير السريع للتطبيقات Rapid Application Development (RAD). وهي منهجية لتطوير البرمجيات تعتمد

على استخدام الحد الأدنى من أساليب التخطيط والنماذج المبدئية لإطلاق النسخة أو الإصدار الأولي، ومن ثم يتم ضبطه وتعديله حتى ينال استحسان الجميع. وينظر كل من المستخدمين ووحدة تقنية المعلومات إلى هذا الإصدار للنموذج المبدئي ويقومون بإجراء المزيد من التغييرات ليصلوا في نهاية المطاف إلى التطبيق النهائي. إن هذا القصور في التخطيط المسبق المكثف بشكل عام يسمح بكتابة البرمجيات بشكل أسرع بكثير ويجعل عملية تغيير المتطلبات أكثر سهولة. يوضح الشكل التوضيحي (١٥-٣) نسخة مبسطة لعملية تطوير البرمجيات القائمة على منهجية التطوير السريع RAD.

شكل توضيحي (١٥-٢)

عملية تحليل المتطلبات الخاصة بتطوير النظم.

• التحضير لتحليل متطلبات النظم: تعيين أعضاء فريق المشروع وجمع المعلومات الأساسية، متضمناً ذلك المجموعات التي قامت بوضع وتحديد هذه المتطلبات وغيرهم من مجموعات المستخدمين المحتمل مشاركتهم في هذه العملية للسماح بجمع وتحليل متطلبات النظام.
• تحديد متطلبات الأعمال: تحديد كل المتطلبات سواء كانت داخل النطاق أم خارج النطاق، وتحديد وتوثيق قواعد الأعمال المخطط لها، بالإضافة إلى تحديد الواجهات المحتملة من وإلى التطبيق الجديد.
• تحديد نموذج العمليات. تحديد وتخطيط العمليات الرئيسية للأعمال التي ستتعامل مع التطبيق الجديد المقترح. ثم تجزئة هذه العمليات إلى وظائف رئيسية وفرعية يمكن التحكم بها حتى نصل إلى حد لا يمكن فيه تقسيمها أكثر من ذلك.
• تحديد نموذج بيانات منطقي: فهم ونمذجة البيانات بشكل منطقي لدعم التطبيق المقترح. وتحديد كيانات التطبيق وعلاقاتها بالكيانات الأخرى، هذا بالإضافة إلى تحديد السمات أو الحقول التي تتوافق مع الأعمال.
• تحقيق التوافق بين متطلبات الأعمال والنموذج: يجب على فريق المشروع التأكد من أن كلاً من العملية التي تم تعريفها والنموذج المنطقي للبيانات يستوعب جميع المتطلبات وقواعد العمل.
• وضع المواصفات الوظيفية: لا بد من دمج الواجهات الأمامية والعمليات والبيانات لكي تصف بشكل نظامي كيف يمكن للمستخدم المحتمل أن يستخدم النظام وكيف يمكن استرجاع ومعالجة وتخزين البيانات المرتبطة.

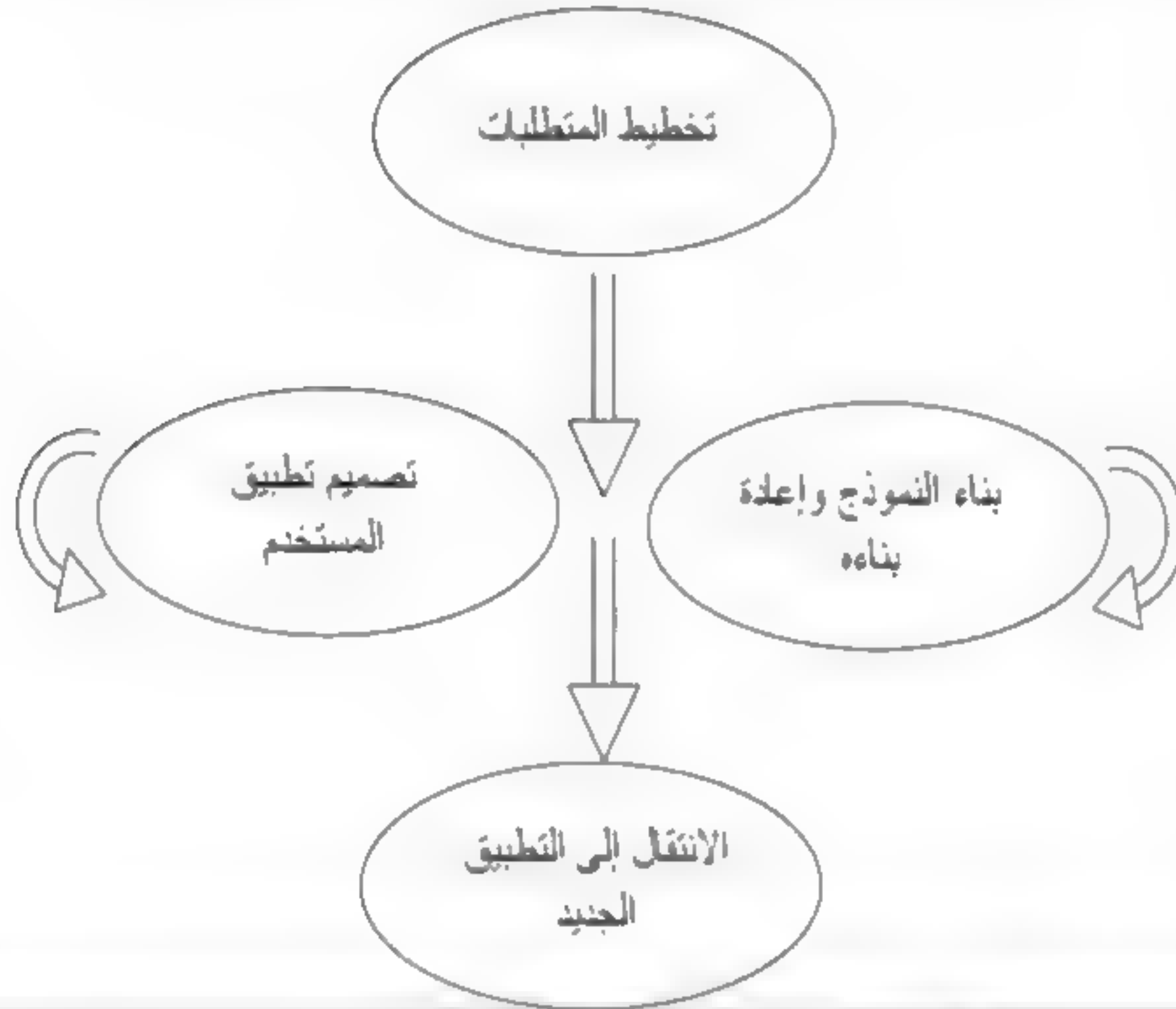
تبدأ عملية التطوير السريع للتطبيقات RAD بتطوير النماذج الأولية للبيانات وعمليات الأعمال لتتمكن من تحديد المتطلبات الأولية. ويمكن إصدار عينة أو نموذج مبدئي من التطبيق باستخدام واحدة من الأدوات البرمجية القوية المتخصصة بإنشاء التقارير هذه الأيام. ومن ثم يتم فحص هذا النموذج مقابل المتطلبات الموجودة حتى يتسنى إدخال التحسينات اللازمة على نماذج البيانات والعمليات. هذه المراحل تتكرر بشكل دوري؛ فهناك مزيد من مخرجات التطوير موجودة في بيان شامل يجمع متطلبات الأعمال والتصميم التقني ليتم استخدامها في بناء نظم جديدة.

يترتب غالباً على أساليب التطوير السريع للتطبيقات RAD تقديم تنازلات على مستوى الأداء الوظيفي وأداء التطبيق بشكل عام في مقابل تمكين تطوير أسرع وتسهيل صيانة التطبيق. تتكون عملية التطوير السريع للنظم من المراحل الأربع التالية:

١- **مرحلة تخطيط المتطلبات في RAD:** يجب على تقنية المعلومات في المؤسسة أن تستخدم بعض العناصر نفسها الموجودة في مراحل تخطيط وتحليل النظم للعملية التقليدية الخاصة بدورة حياة تطوير النظم SDLC الموضحة في الشكل التوضيحي (١٥-٢). في جميع الأحوال، ووفقاً لأسلوب التطوير السريع للتطبيقات فإنه يتعين على المستخدمين، والمديرين، وأعضاء فريق تقنية المعلومات، مناقشة متطلبات الأعمال، ونطاق المشروع، والقيود، ومتطلبات النظام والموافقة عليها. تنتهي هذه المرحلة عندما يتفق الفريق على القضايا الرئيسية والحصول على تصريح من الإدارة بالاستمرار.

شكل توضيحي (٣-١٥)

عملية تطوير البرمجيات وفقاً لأسلوب التطوير السريع للتطبيقات RAD



٢- مرحلة تصميم تطبيقات المستخدم في RAD: في هذه المرحلة يعمل المستخدمون مع محلي النظم على وضع النماذج والنماذج الأولية التي تمثل جميع عمليات ومدخلات ومخرجات النظم. وتقوم عادة المجموعات الرئيسية والفرعية المشاركة في عملية التطوير السريع للتطبيقات RAD باستخدام أدوات تطوير التطبيقات الموجودة في إدارة تقنية المعلومات لترجمة احتياجات المستخدم إلى نماذج عمل. وتعد مرحلة تصميم تطبيقات المستخدم عملية تفاعلية مستمرة فهي تسمح للمستخدمين بفهم وتعديل نموذج العمل الخاص بالنظام الذي يلبي جميع احتياجاتهم.

٣- مرحلة البناء: تركز هذه المرحلة على مهام تطوير برامج وتطبيقات مشابهة لعملية دورة حياة تطوير النظم SDLC. وطبقاً لنهج التطوير السريع للتطبيقات، فإنه ومن ناحية

أخرى، يستمر المستخدمون في المشاركة واقتراح التعديلات والتحسينات عند التطوير الفعلي للشاشات والتقارير. وتتمثل مهام هذه المرحلة في البرمجة وتطوير التطبيقات، وكتابة التعليمات البرمجية، وتكامل الوحدات واختبار النظام.

٤- **مرحلة الانتقال في RAD:** تشبه هذه المرحلة الأخيرة المهام الأخيرة الموجودة في تطبيق دورة حياة تطوير النظم SDLC بما فيها تحويل البيانات والاختبار والتحول إلى النظام الجديد وتدريب المستخدمين. وبالمقارنة مع الطرق التقليدية، فإنه يتم ضغط العملية برمتها. ونتيجة لذلك، فإنه يتم بناء النظام الجديد وتسليمه ووضع موضع التشغيل بشكل أسرع بكثير. فمهام هذه المرحلة هي تحويل البيانات واختبار النظام بأكمله وتحويل النظام وتدريب المستخدمين.

لقد بدأ نهج التطوير السريع للنظم RAD الخاص بتطوير النظم في الوقت الذي بدأت فيه المؤسسات وإدارات تقنية المعلومات التابعة لها في الانتقال من نظم الحاسبات المركزية القديمة إلى نظم العميل-الخادم، وذلك أثناء زيادة هيمنة نظم الحاسبات المحمولة والحاسبات المكتبية، والأكثر أهمية من ذلك هو ظهور الإنترنت. وبالعودة إلى أيام دورة حياة تطوير نظم SDLC الخاصة بالحاسبات الكبيرة المركزية، فقد عبر العديد من مستخدمي تقنية المعلومات داخل المؤسسة وقتها عن استيائهم من عمليات التطوير البطيئة وفشل النظم الجديدة والميزانيات المهدرة ومجموعة من المشاكل الأخرى. إن تقديم أدوات التطوير السريع للتطبيقات RAD إلى مستخدمي النظم هؤلاء كان أشبه بالتجلي. فقد تمكنوا من إلقاء نظرة سريعة على إصدارات النماذج الأولية لتقارير وحتى عمليات النظم ومن ثم استطاعوا المضي قدماً من خلال الإصدار السريع والفعال لنهج التطوير السريع للتطبيقات RAD.

ونظراً لسهولة استخدامها، فإن المؤسسات التي تشجع على استخدام أدوات التطوير السريع للتطبيقات RAD قد تجد نفسها في مشاكل تتعلق بالأمن والضوابط الداخلية للتطبيقات في حال استخدمت نهج التطوير السريع للتطبيقات RAD بشراسة لتطوير التطبيقات الجديدة دون وضع الضوابط الملائمة على التطبيقات

الجديدة. الشكل التوضيحي (١٥-٤) يوجز لنا بعض ضوابط وإجراءات حوكمة تقنية المعلومات التي لا بد من وجودها في المحيط الذي تُستخدم فيه عمليات التطوير السريع للتطبيقات RAD.

تقوم العديد من المؤسسات هذه الأيام بتطوير تقاريرها الخاصة بها والتي يتم إنشاؤها حسب الطلب لدعم تطبيقات البرمجيات التي تم شراؤها. ويتم اليوم تطوير تطبيقات البرمجيات التي يتم شراؤها بصورة شبه دائمة باستخدام أداة خاصة لإنشاء التقارير أو باستخدام إحدى أدوات التطوير السريع للتطبيقات الخاصة بهذه البرمجية. ويمكن تطبيق أفضل ممارسات حوكمة تقنية المعلومات التي تمت مناقشتها في هذا الفصل على جميع هذه الأدوات.

تخطيط موارد المؤسسة وعمليات حوكمة تقنية المعلومات:

يتم عادة توظيف أحد قواعد البيانات الشاملة للعمل على أنه مستودع للبيانات، حيث تعمل نظم تخطيط موارد المؤسسة (ERP) على تكامل المعلومات الإدارية الداخلية والخارجية عبر المؤسسة بالكامل حيث تشتمل على نظم الإدارة المالية، وإدارة التصنيع عند الحاجة، وإدارة المبيعات والخدمات وإدارة علاقات العملاء وغير ذلك. وتعد نظم ERP من قواعد البيانات المعقدة التي تعمل على أتمتة هذا النشاط من خلال تطبيقات البرمجيات المتكاملة. حيث إن الغرض من هذه النظم هو تسهيل تدفق المعلومات بين جميع وحدات الأعمال داخل حدود المنظمة وإدارة الاتصالات مع أصحاب المصالح الخارجيين. إذاً فالهدف من نظام ERP هو تحسين وتبسيط العمليات الداخلية للأعمال، والذي يتطلب عادة إعادة هندسة العمليات الحالية لتلك الأعمال.

شكل توضيحي (١٥-٤)

ضوابط وإجراءات حوكمة تقنية المعلومات المتعلقة بالتطوير السريع للتطبيقات RAD.

إن التطوير السريع للتطبيقات RAD هو أسلوب لتطوير البرمجيات. حيث يركز على فترات زمنية قصيرة للتطوير (من ٣٠ إلى ٩٠ يوماً). وهذا الأسلوب لا يصلح في تطوير التطبيقات المعقدة أو التطبيقات التي تعالج كميات كبيرة من المعاملات بشكل سريع مثل البيئات الخاصة بمعالجة الدفعة. وقد يكون من المناسب بالنسبة للمؤسسة أن تستخدم هذا الأسلوب لتطوير أو إعادة تصميم التطبيقات ذات المخاطر المنخفضة أو التطبيقات الأقل تعقيداً مثل مواقع الويب (الإنترنت) ذات المعاملات التي لا تحتوي على طاقة إنتاجية عالية المستوى Throughput. إضافة إلى ذلك، واستناداً إلى درجة تحمل المؤسسة للمخاطر وتحديد المهام الحساسة والدرجة للتطبيق، فإنه يتحتم على المؤسسة استخدام الضوابط والإجراءات الخاصة بحوكمة تقنية المعلومات لضمان توظيف الأساليب المناسبة الخاصة بالتطوير السريع للتطبيقات RAD أثناء مراحل التصميم والتطوير للتطبيق الجديد في تقنية المعلومات ضمن منهجية تطوير مهيكلية. والنقاط التالية توجز بعض الضوابط والإجراءات العامة والجيدة في حوكمة تقنية المعلومات:

- اختر أداة مناسبة لتوليد تقارير التطبيقات بحيث تكون مرنة وتلبي احتياجات تطبيقات الأعمال. كما يتعين على الإدارة ضمان أن أسلوب التطوير الذي تم اختياره مناسب لإدارة تعقيدية ومخاطر التطبيقات التي بصدد تطويرها.

- ضع قواعد لتقنية المعلومات مثل أنه سيتم فقط استخدام تقنية التطوير السريع للتطبيقات RAD التي تمت الموافقة عليها لأغراض التطبيقات الإنتاجية ما لم تكن هناك موافقة محددة من الإدارة العليا لتقنية المعلومات.

- نفذ برامج تدريبية أولية ومستمرة لكادر تقنية المعلومات والمستخدمين المعنيين تتعلق باستخدام الأداة البرمجية التي تم اختيارها للتطوير السريع لتطبيقات RAD.

- ضع معايير خاصة بإدارة تقنية المعلومات فيما يتعلق بالتطبيقات المطورة خلال عمليات التطوير السريع للتطبيقات RAD والتي تضم المراحل الرسمية للبدء، والتطوير، والتنفيذ. حيث تتطلب الفترة الزمنية القصيرة لمشاريع التطوير السريع للتطبيقات RAD ضرورة الإسراع في تحديد المتطلبات الوظيفية التي يجب أن تبقى إلى حد كبير دون تغيير أثناء عملية التطوير.

<p>• حدّد أي المستويات المناسبة من العاملين والمستخدمين النهائيين في تقنية المعلومات هم الذين سيتم تعيينهم في مشاريع التطوير السريع للتطبيقات لبناء وتعديل التصميمات. أما بالنسبة لمشاريع التطوير السريع للتطبيقات الأكبر حجماً، فإنه يجب تعيين المتخصصين كمديري قواعد البيانات، وفنيي الشبكات ومبرمجي النظم ليكونوا مسؤولين عن القرارات الرئيسية المتعلقة بالتطوير السريع للتطبيقات RAD.</p>
<p>• لا بد من وجود معايير وضوابط للتطوير السريع للتطبيقات RAD في المؤسسة للتأكد من:</p> <ul style="list-style-type: none"> - أن الإدارات تستخدم أساليب التطوير السريع للتطبيقات RAD فقط إذا اقتضت الحاجة ذلك. - أن الإدارة تشتمل على الخصائص الأمنية والرقابية في جميع التطبيقات المطورة. - أن موظفي ضمان الجودة يقومون بفحص ما إذا كانت السمات الأمنية والرقابية (التي تتناسب مع مستويات المخاطر) موجودة وموظفة كما يجب أم لا. - أن المستخدمين النهائيين يشاركون بشكل مناسب خلال مشروعات التطوير السريع للتطبيقات RAD. - أن مديري المشروعات يراقبون عن كثب وعن قرب جميع أنشطة المشروع.
<p>• قم بتحديد ما إذا كانت جميع التطبيقات التي تم تطويرها باستخدام التطوير السريع للتطبيقات قد تم توثيقها بالشكل المناسب أم لا، وأن عملية التوثيق قد تمت بالتوازي مع عملية تطوير التطبيق. ومن خلال الإنتاج المتزامن للوثائق ودون زيادة الوقت المخصص لتطوير التطبيق، فإن التطبيقات المطورة بتقنية التطوير السريع للتطبيقات RAD ستسهم في توفير الوقت أثناء عمليات الصيانة المستقبلية للنظام.</p>
<p>• قم بوضع مبادئ صارمة فيما يخص قواعد التسمية أو كتابة الجمل البرمجية بحيث يتمكن مطور تطبيقات RAD بشكل شبه دائم من فهم نص شيفرة المصدر Source Code الخاصة بمولد التطبيقات الذي يتم توليده من قبل أحد محترفي التطوير السريع للتطبيقات RAD أو غيره من محترفي تقنية المعلومات.</p>

يمكننا التأمل في وظائف نظام ERP من خلال عملية التصنيع، حيث يحتاج أحد أجزاء المنتج إلى تصميم، وطلب الموارد اللازمة لبناء هذا الجزء، ووضع العمليات الخاصة بحساب تكلفة وتسويق هذا الجزء، حيث يتم تنفيذ طلبات شراء المواد، وتبدأ عملية الإنتاج، ومن ثم يأتي دور التدفق الكلي لعمليات الإنتاج والعمليات التشغيلية فيما يتعلق باستقبال أوامر الشراء من العميل، والشحن، وإصدار الفواتير الخاصة بهذا العنصر. إن هذه العمليات وغيرها تنطوي على سلسلة من أنشطة مستقلة إلا أنها مرتبطة فيما بينها بعلاقات متبادلة،

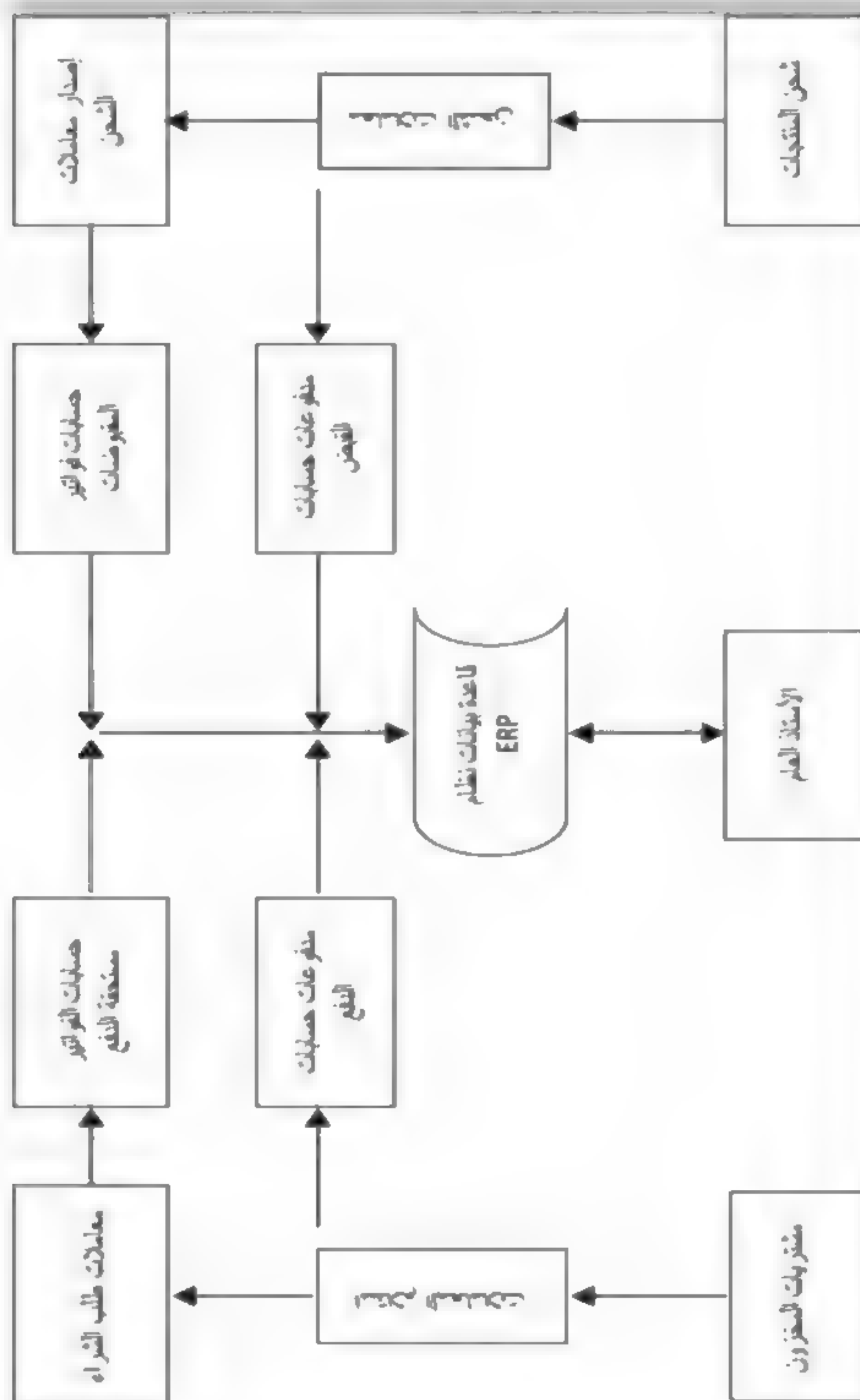
حيث كانت تدار في السابق عن طريق مجموعة منفصلة من تطبيقات تقنية المعلومات مثل التطبيقات الخاصة بتلقي الطلبات ومراقبة المخزون وجدولة الإنتاج والشحن وحساب المقبوضات وغيرها الكثير. في حين يقوم نظام ERP بربط جميع هذه الأنشطة وأكثر في سلسلة مترابطة بإحكام من وظائف قاعدة البيانات.

يحاول نظام ERP أن يعمل على تكامل كل الأقسام والإدارات في الشركة ليضعها في نظام حاسب آلي واحد يمكنه خدمة وتلبية الاحتياجات الخاصة بجميع الأقسام التابعة لها. وقد يكون هذا أمراً صعباً، أن يتم بناء نظام برمجي واحد يلبي حاجات الناس في الأمور المالية بالإضافة إلى الموارد البشرية والمستودعات. فقبل ظهور نظام ERP، عادة ما كان لكل قسم من هذه الأقسام نظام حاسب آلي خاص به مُطَوَّر بوسائل خاصة بحيث يستطيع القسم أن يقوم بأداء الأعمال الخاصة به، إلا أن نظام ERP قد قام بدمج هذه النظم جميعاً في نظام برمجي واحد متكامل يدار من قبل قاعدة بيانات واحدة، بحيث يسمح للأقسام المختلفة بمشاركة المعلومات والاتصال فيما بينهم بسهولة. قد يكون لهذا النهج التكاملي مردود واسع إذا ما قامت الشركات بتثبيت البرمجية بشكل سليم.

يوجد العديد من الطرق لوصف نظام ERP. إلا أن الشكل التوضيحي (١٥-٥) يعرض لنا وصفاً لتدفق البيانات المحاسبية الأساسية الخاصة بأعمال إحدى المؤسسات. وتتضمن أوامر الشراء وحساب المدفوعات وغيرها من العمليات التقليدية لنظم الأعمال التي ستكون جزءاً من نظام ERP. هذه العناصر تعد من متطلبات النظم اللازمة لبناء أحد أجزاء عملية التصنيع والتي تم وصفها مسبقاً. فقد كانت هذه العناصر عبارة عن عمليات نظم تقليدية منفصلة لكل منها بيانات وملفات معاملات رئيسية خاصة بها، وتستطيع الاتصال بتطبيقات أخرى كنظام الأستاذ العام. وعلى الرغم من أن هذا الشكل يعرض سلسلة من عمليات توزيع الإنتاج كالوظائف التقليدية لحساب المقبوضات، وحساب المدفوعات، فإن التطبيق الكامل لنظام ERP الخاص بالمؤسسة يحتوي على مجموعة أكبر بكثير من النظم الأخرى كالتسويق والموارد البشرية، إذ يتم ربط جميع النظم معاً بإحكام من خلال توصيفات وروابط مشتركة للبيانات.

شكل توضيحي (١٥-٥)

مثال على بنية نظام تخطيط موارد المؤسسة ERP



قد يتساءل المدير الأول عن سبب تأخير وصول معلومات شكاوى العملاء القادمة من نظام مرتجعات المنتجات. وقد يحتج أعضاء آخرون في الكادر الوظيفي من أنه يجب عليهم إعادة إدخال المعاملات نفسها في تطبيقات مختلفة ولكنها مترابطة. في أغلب الأحيان يبدو أن قاعدة البيانات المدمجة المشتركة - نظام ERP - هي الحل الأسهل هنا. من ناحية أخرى، فإن عملية تطبيق نظام ERP ليس بالخطوة السهلة أو الصغيرة. حتى في أحسن الظروف فإن هذا النظام سيستهلك كميات كبيرة من وقت وموارد المؤسسة. كما يجب أن يكون هناك مشاركة فعالة من المديرين الرئيسيين وأعضاء فريق تقنية المعلومات وحتى أصحاب المصلحة الآخرين.

من منظور حوكمة تقنية المعلومات فإنه يوجد نقاط رئيسية يجب أن يتم أخذها في الاعتبار عند تطبيق نظام قاعدة بيانات ERP في المؤسسة، وهي:

- **تحديد أهداف ومتطلبات نظام ERP:** يعتبر هذا المفهوم جديداً نسبياً في نظم تقنية المعلومات، إذ هناك الكثير من الدعاية المنشورة حول ما يمكن أن تحققه قواعد البيانات الشاملة لنظام تخطيط الموارد المؤسسية. فضلاً عن أنه بالاستناد إلى المعرفة التي لديهم فيما يمكن أن تحققه قواعد البيانات الشاملة لنظام تخطيط الموارد المؤسسية، يجب على المبادرين في المشروع وضع أهداف ومتطلبات قوية للمشروع الجديد الخاص بتطبيق نظام تخطيط الموارد المؤسسية ERP.

- **بناء فريق المشروع من جميع الإدارات:** إن قاعدة البيانات الخاصة بتخطيط موارد المؤسسة تعد أكثر من مجرد نظام جديد في تقنية المعلومات، وإنما ينطوي تحته العديد من أعضاء المؤسسة. لذا يجب تعيين فريق من جميع الوظائف المختلفة لتقنية المعلومات وأعضاء من مجتمع المستخدمين لقيادة المشروع القادم والخاص بتخطيط الموارد المؤسسية.

- **تقدير متطلبات التكلفة والوقت اللازمة لتطبيق نظام ERP:** بالنسبة للمؤسسة المكونة من وحدة أعمال واحدة فقط ويعمل بها ما بين ٢٥ إلى ١٠٠٠ موظف، قد تحتاج إلى حزمة أصغر من برمجية قاعدة بيانات ERP تُكلف نحو ٢٥٠٠٠٠ دولار أمريكي. في حين أن المؤسسات الكبيرة المتعددة وحدات الأعمال ويعمل بها عدد من المستخدمين

قد يصل إلى ٥٠٠٠ مستخدم، ربما يكلف البرنامج الأساسي لنظام ERP نحو مليوني دولار أمريكي. كما يجب على المؤسسة أن تضع توقعات حقيقية وواقعية لمتطلبات الوقت اللازم لهذا المستوى من المشروع، وأن يفترضوا أن مثل هذا المشروع الكبير لتقنية المعلومات يحتاج إلى سنة واحدة على الأقل.

• **اختيار أحد المنتجات البرمجية لنظام ERP:** هناك عدد كبير من الباعة يقدمون برنامج نظام تخطيط الموارد المؤسسية ERP. فهناك مزودو برمجيات رئيسيون أمثال ساب SAP، أوراكل Oracle، وميكروسوفت Microsoft. هذا بالإضافة إلى بعض الباعة الأقل شهرة مثل إبيكور Epicor. ولتجنب سلسلة الاجتماعات أو اللقاءات اللانهائية مع البائعين والمواد الترويجية اللامعة، فإنه يجب على الفريق المنوط به عملية الاختيار الوقوف بحزم على الأهداف المحددة للمتطلبات والميزانية وعلى البيئة البرمجية الحالية للمؤسسة كذلك. ويتعين على أي بائع لمنتج برنامج ERP قابل للتطبيق أن يكون قادراً على تقديم نسخة تجريبية تمثل منتج ERP الخاص بهم.

• **تطبيق أساليب منهجية لإدارة المشاريع لتطبيق نظام ERP:** يتحدث الفصل السادس عشر من هذا الكتاب عن تقنيات التخطيط الرسمية للمشاريع والبرامج. ونظراً لأن تطبيق نظام ERP يعتبر مهمة كبيرة، فإنه يجب على المؤسسة أن تضع وتتبع منهجيات رسمية لتخطيط المشاريع من أجل تطبيق نظام ERP الذي نسعى إليه.

• **إنشاء قاعدة بيانات تجريبية لنظام ERP والبدء في التنفيذ المرحلي:** بمجرد أن يعمل تطبيق ERP في المؤسسة على أكمل وجه فإنه سيؤثر في عدد كبير من التطبيقات التقليدية. على كل حال، يجب الحرص على إطلاق التطبيق المرحلي على أساس تطبيق بعد الآخر، وذلك باستخدام قاعدة بيانات تجريبية أعدت في مراحل سابقة للمشروع.

• **تقديم تدريب مكثف للمستخدمين:** قد ينطوي التطبيق الجديد لنظام ERP على أشكال جديدة للمعاملات وغيرها من التغيرات التي تطرأ على النظم والتي تكون في بعض الأحيان صغيرة لكنها فنية. وفي جزء من خطة المشروع وفي إحدى مسؤوليات أعضاء فريق تطبيق نظام ERP، يجب أن يكون هناك برنامج تدريبي قوي للمستخدمين.

• **إقرار ميزانيات المشرع ومراقبة حثيثة لتكاليف نظام ERP:** بعيداً عن رسوم الترخيص الخاصة بقاعدة البيانات التي تم اختيارها، فإن مشروع نظام ERP يعد من المشاريع الباهظة الثمن بالنسبة للمؤسسة. لذا يُطلب من أعضاء فريق المشروع وغيرهم من الأشخاص المشاركين في هذا العمل أن يقوموا بتسجيل عدد ساعات العمل الخاصة بهم فضلاً عن تحميل أي مصروفات مباشرة على مشروع نظام ERP. ولابد من مراقبة هذه المصروفات التي يتم تحميلها على المشروع ويتم المطالبة بها عن كثب والمساءلة بشأنها إذا اقتضى الأمر. في جميع الأحوال، ولعل أحد نقاط القلق الرئيسية بالنسبة لحوكمة تقنية المعلومات، والتي ربما تكون بمثابة مشكلة في بعض الأحيان عندما يقوم أعضاء الفريق بتحميل ساعات عملهم على المشروع حتى لو لم يقوموا بالفعل بتنفيذ أنشطة مرتبطة مباشرة بالمشروع.

• **وضع إستراتيجية للخروج إذا اقتضت الضرورة ذلك:** يمكن أن يسفر تطبيق نظام ERP الذي تم تخطيطه وتنفيذه بشكل جيد عن بعض المزايا الرئيسية الملموسة وغير الملموسة بالنسبة للمؤسسة. إلا أنه في بعض الأحيان قد تكون هناك أمور تسير على نحو خاطئ. على سبيل المثال، بعض سمات البرمجيات الخاصة ببائعي قاعدة بيانات ERP قد لا تعمل كما تم التعهد به أو كما كان متوقعاً. فقد يكون هناك مشاكل تقنية في شاشات النظم أو أي مجموعة أخرى من المشاكل المحتملة. فكما يقول التعبير القديم، لا تهدر المال الصالح في إصلاح ما تلف، فإنه يجب على فريق العمل أن يضع إستراتيجية خروج لئلا يؤول أعمال المشروع بشكل لطيف والعودة إلى العمليات التشغيلية التقليدية لتقنية المعلومات والأعمال.

شكل توضيحي (٦-١٥)

المزايا الملموسة وغير الملموسة الناتجة عن تطبيقات نظام ERP في المؤسسة.

المزايا الملموسة لنظام ERP:

- تخفيضات المخزون.
- تقليص أعداد الموظفين.
- تحسينات في إدارة النظام.
- تبسيط الروابط.
- تحسينات في دورة الإقفال المالي.
- تخفيض تكاليف تقنية المعلومات.
- تقليص تكلفة المشتريات.
- تحسينات في الإدارة النقدية.
- تقليل صيانة تقنية المعلومات والنظم.
- نظم محسنة تسلم في الوقت المحدد.

المزايا غير الملموسة لنظام ERP:

- وصول ورؤية أكبر لمعلومات النظم.
- عمليات محسنة جديدة.
- استجابات أكبر للعملاء.
- توحيد النظم والعمليات.
- تحسينات في سلسلة طلبات التوريد.

بالرغم من التصريحات التحذيرية السابقة، فإن التطبيق الناجح لنظام ERP قد يعود على المؤسسة ببعض المزايا الملموسة وغير الملموسة. كما هو موضح في الشكل التوضيحي (٦-١٥). يمكن أن يكون تطبيق نظام ERP أحد المشروعات الكبيرة في المؤسسة والذي يمكن

أن يعود عليها بالعديد من الفوائد. وكما ناقشنا أهمية العمليات القوية لحوكمة تقنية المعلومات بالنسبة لكل من عمليات دورة حياة تطوير النظم SDLC وعمليات التطوير السريع للتطبيقات RAD، فإن هذه القضايا تعد غاية في الأهمية عندما نقوم بإطلاق نظام قاعدة بيانات تخطيط الموارد المؤسسية ERP داخل المؤسسة.

الفصل السادس عشر

قضايا حوكمة تقنية المعلومات: إدارة المشاريع والبرامج

على الرغم من استخدام المؤسسات للهياكل التنظيمية الرسمية من أجل إدارة معظم الأنشطة الخاصة بها، فإن هناك مجموعة كبيرة من أنشطة المؤسسة التي يتم تنظيمها وإدارتها على شكل مشاريع. ويُستخدم مصطلح المشروع في الأنشطة العلمية، والحكومية، وحتى في الأنشطة المدرسية، وهو عبارة عن نشاط تعاوني يتم داخل المؤسسة ويشتمل على نشاطات كالأبحاث أو تطوير نظم تقنية المعلومات. ويتم تخطيط المشاريع بشكل خاص من أجل تحقيق هدف معين على خلاف الأنشطة الاعتيادية للمؤسسة. وتُعرف المشاريع عادة بأن لها هيكلًا تنظيميًا مؤقتًا وليس دائمًا. وهي تتكون من فرق من داخل أو خارج الإدارات لإنجاز مهام محددة في أوقات محددة.

يتم تنظيم وإدارة العديد من أعمال تطوير نظم تقنية المعلومات على هيئة مشاريع، فعندما تبدأ المؤسسة أو وحدة تقنية المعلومات التابعة لها في سلسلة من المشاريع المختلفة وفي الوقت نفسه يوجد بينها أوجه تشابه، فإن هذه المجموعات من المشاريع يطلق عليها اسم برامج Programs. وفي أغلب الأحيان تعد المشاريع والبرامج وسائل فعالة لإدارة وتطبيق التغييرات التي تطرأ على نظم وعمليات تقنية المعلومات، إلا أنها قد تتسبب أيضاً في وجود بعض المشاكل المتعلقة بالحوكمة والرقابة، وذلك لكونها مجهودات تتخطى عادة الحدود التنظيمية الاعتيادية، فهي تحتاج إلى آليات خاصة لمتابعة وضبط المشاريع.

سيتناول هذا الفصل التقنيات الفعالة لإدارة المشاريع والبرامج بهدف تحسين الحوكمة الشاملة لتقنية المعلومات. وسنقوم بتقديم المعايير الخاصة بالدليل المعرفي لإدارة المشاريع (PMBOK) Project Management Book of Knowledge الصادرة عن معهد إدارة المشاريع (www.pmi.org) Project Management Institute (PMI) كما سنناقش أيضاً، لماذا يعد الامتثال لهذه المعايير من الأمور الهامة بالنسبة للإدارة الفعالة للمشاريع والبرامج؟

عملية إدارة المشاريع:

يتم استخدام مصطلح المشروع غالباً على نحو غير سليم هذه الأيام في العديد من العمليات التشغيلية الخاصة بتقنية المعلومات وغيرها من الأعمال المؤسسية. فكثيراً ما يُطلب من مطوري تطبيقات تقنية المعلومات أو غيرهم من الأشخاص العاملين في مجالات أخرى داخل المؤسسة أن يقوموا بإعداد مشروع لتنفيذ بعض الأعمال المحددة. وكان المقصود من الجهود الخاصة بإعداد مثل هذا المشروع والتخطيط له تخصيص أشياء مختلفة لأشخاص مختلفين. وتقتضي هذه الجهود غالباً قيام القائد المعين باستدعاء الفريق المكلف بالمشروع للاجتماع وعمل ما هو أكثر بقليل من مجرد قول، "أريدك أنت وأنت وأنت" لتنفيذ مهام المشروع المختلفة. ولم تكن الخطوات الضرورية اللازمة لتنظيم المشروع والتخطيط له تحظى بالاهتمام الكافي. ولهذا كانت هذه الجهود غير الرسمية "للمشروع" تؤول غالباً إلى الفشل بسبب عدم فهم الفريق المكلف بالمشروع لحقيقة الدور المنوط به وعدم إلمامه بالأهداف العامة للمشروع، هذا بالإضافة إلى أن المتطلبات الخاصة بوقت ونطاق المشروع لم تكن محددة. وقد أدت هذه الجهود في كثير من الأحيان إلى فشل المشاريع بسبب تجاوز الوقت والميزانية أو للعديد من الأسباب الأخرى. كان سبب هذا الإخفاق غالباً هو الافتقار إلى نهج منظم ومتناغم لإدارة المشاريع.

وقد استمرت إدارة المشاريع في كونها مجرد مفهوم تم تعريفه بشكل ضعيف وغير واضح حتى منتصف تسعينيات القرن الماضي. فعلى الرغم من وجود العديد من الأساليب الجيدة المعمول بها في ذلك الوقت في مشاريع البنية التحتية كبناء الجسور على الطرق السريعة، فإن تلك الحقبة قد شهدت العديد من الإخفاقات في تطوير نظم تقنية المعلومات. باستثناء بعض الأساليب التي كانت تقودها الولايات المتحدة الأمريكية لتحسين تلك المشاريع الخاصة بتطوير تقنية المعلومات، حيث لم يكن هناك نهج ثابت لإدارة المشاريع على مدى عدة سنوات. إلا أن الأمور قد تغيرت عندما تم تأسيس معهد إدارة المشاريع PMI، والذي بدأ بمجموعة صغيرة من المهنيين المتخصصين الأمريكيين الذين يبحثون عن تعريف أكثر انسجاماً مع أعمالهم. واعتباراً من عام ٢٠١٢ أصبح معهد إدارة المشاريع PMI منظمة مهنية دولية تضم في عضويتها نحو ٦٠٠٠٠٠ شخص بين عضو ومدير مشاريع معتمد من قبل المعهد في ١٨٥ دولة. وقد قام معهد إدارة المشاريع PMI ببحث وتطوير ونشر مجموعة كبيرة من المواد الإرشادية المتعلقة بإدارة

المشاريع. ومن أهم المطبوعات الصادرة عن هذا المعهد الوثيقة الأشبه بالمعايير والتي أُطلق عليها كتاب الدليل المعرفي لإدارة المشاريع PMBOK^(١). وهو بمثابة دليل لجميع الجوانب الخاصة بإدارة المشاريع. وقد أصبح الدليل المعرفي لإدارة المشاريع PMBOK أحد المعايير المهنية للممارسات الخاصة بإدارة المشاريع في جميع أنحاء العالم.

يعرض الشكل التوضيحي (١٦-١) تعريف المشروع طبقاً للدليل المعرفي لإدارة المشاريع PMBOK. وعلى الرغم من أن هذا الدليل يتسم إلى حد ما بالإسهاب وربما يكون عاماً وشاملاً فقط للإرشادات المتعلقة بحوكمة تقنية المعلومات، فإنه قام بتعريف المشروع على أنه جهد مؤقت له تاريخ بداية ونهاية معلوم وأهداف وغايات محددة. وتتخطى المشاريع غالباً الحدود التنظيمية الاعتيادية وتعمل بشكل منفصل نوعاً ما، أو خارج الإطار الطبيعي لإجراءات الإدارة أو المؤسسة. وقد يتم تخصيص فريق للمشروع مكون من أشخاص ينتمون إلى وحدات تنظيمية مختلفة في المؤسسة، ويتم تقديم التقارير على أساس الخط النقطي (نمط العلاقة الضعيفة بين الموظف ورئيسه) لمدير مشروع مستقل. في بعض الأحيان، قد يعمل فريق عمل المشروع بدوام جزئي في المشروع مع استمرار تحملهم لمسؤولياتهم تجاه وظائفهم الاعتيادية. ونظراً لأن أنشطة المشروع تتخطى غالباً الحدود التنظيمية ويتم تشغيلها كأعمال منفصلة ومستقلة، ومن ثم قد تكون هناك مشاكل تتعلق بقضايا حوكمة تقنية المعلومات ما لم تكن هناك معايير قوية ومتسقة معمول بها لإدارة المشاريع.

إضافة للإرشادات الخاصة بالدليل المعرفي لإدارة المشاريع والتي تتحدث عن المشاريع المستقلة القائمة بذاتها، فإن لدى معهد إدارة المشاريع PMI أيضاً المزيد من المواد الإرشادية والتوجيهية الخاصة بإدارة البرامج والمحافظة. وسيتم الحديث عنها في الأقسام اللاحقة. حيث تشير إدارة البرامج بشكل عام إلى سلسلة من المشاريع المرتبطة ببعضها. في حين تشمل إدارة المحافظة معايير خاصة بمجموعة المشاريع والبرامج داخل المؤسسة. كما أن لدى معهد إدارة المشاريع PMI أيضاً برنامج الشهادة الاحترافية لمديري المشاريع، حيث يتم اعتماد الأعضاء الذين يجتازون الاختبارات المهنية لهذا البرنامج بنجاح ويحققون متطلبات الخبرة كمدير مشروعات محترف (PMP) Project Management Professional. وقد أصبح معهد إدارة المشاريع PMI والدليل المعرفي لإدارة المشاريع PMBOK الصادر عنه

من المعايير العملية بالنسبة للعديد من أنشطة إدارة المشاريع في المؤسسات سواء في الولايات المتحدة الأمريكية أم في جميع أنحاء العالم.

شكل توضيحي (١-١٦)

تعريف المشروع وفقاً للدليل المعرفي لإدارة المشاريع PMBOK

المشروع هو مسعى مؤقت يتم القيام به من أجل تقديم منتج أو خدمة أو نتيجة فريدة من نوعها. تشير الطبيعة المؤقتة للمشاريع إلى وجود بداية ونهاية واضحة. ويتم الوصول إلى النهاية عندما تتحقق جميع أهداف المشروع أو عندما يتم إنهاء المشروع بسبب عدم إمكانية تحقيق أهداف المشروع أو عندما لا يعود هناك حاجة إلى المشروع. وليس بالضرورة أن تشير كلمة مؤقت إلى فترات زمنية قصيرة. وعموماً فإن كلمة مؤقت لا تنطبق على المنتج أو الخدمة أو النتيجة التي حصلنا عليها من المشروع. ويتم القيام بمعظم المشاريع لخلق نتائج دائمة. على سبيل المثال، مشروع بناء تمثال أو نصب تذكاري وطني يؤدي إلى نتيجة من المتوقع أن تدوم لعدة قرون. وقد يكون للمشاريع أيضاً آثار اجتماعية واقتصادية وبيئية قد تدوم أكثر بكثير من المشاريع نفسها.

كما أن كل مشروع يعمل على إيجاد منتج أو خدمة أو نتيجة فريدة من نوعها. وعلى الرغم من احتمالية وجود عناصر مكررة في بعض مخرجات المشاريع، فإن هذا التكرار لا يغير سمة التفرد الأساسية لعمل المشروع. على سبيل المثال، يتم تشييد المباني المكتبية من المواد نفسها أو من مواد شبيهة وعن طريق الفريق نفسه، إلا أن كل موقع يختلف ويمتاز عن غيره في التصميم أو الظروف أو المقاولين أو غير ذلك.

إن جهود العمل المستمرة بشكل عام عبارة عن عملية متكررة، ذلك لأنه يسير وفق إجراءات تنظيمية قائمة. وعلى النقيض من ذلك، فإنه نظراً للطبيعة الفريدة للمشاريع، قد تحوم شكوك حول المنتجات أو الخدمات أو النتائج التي يُوجدُها المشروع. فقد تكون مهام المشروع جديدة بالنسبة لأعضاء فريق المشروع، الأمر الذي يتطلب تخطيطاً أكثر تفانياً من غيرها من الأعمال الروتينية. بالإضافة إلى ذلك، فإنه يتم تنفيذ المشاريع على جميع المستويات التنظيمية. وقد يشمل المشروع شخصاً واحداً أو وحدة تنظيمية واحدة أو وحدات تنظيمية متعددة.

يستطيع المشروع إيجاد:

- منتج يمكن أن يكون أحد مكونات عنصر ما أو عنصراً نهائياً بحد ذاته.
- القدرة على أداء خدمة (على أنها إحدى إدارات الأعمال التي تدعم الإنتاج أو التوزيع).
- أو نتيجة مخرج أو وثيقة (على سبيل المثال، أحد المشاريع البحثية التي تُستخدم لتحديد ما إذا كان هناك توجه معين أو عملية جديدة سوف تفيد المجتمع).

تقدم الأقسام التالية مقدمة عامة عن الدليل المعرفي لإدارة المشاريع PMBOK وأهميته باعتبارها أسلوباً أساسياً للتطوير وإدارة المشاريع. لسنا هنا بصدد تقديم وصف تفصيلي لمعايير الدليل المعرفي لإدارة المشاريع PMBOK، بل تقديمها باعتبارها إحدى الأدوات الهامة لحوكمة تقنية المعلومات الخاصة بإدارة المشاريع في المؤسسة. عندما تقوم إدارة تقنية المعلومات في المؤسسة باستخدام تقنيات إدارة المشاريع لتطوير تطبيقات جديدة أو غيرها من عمليات النظم، فلا بد أن يتم هذا التطوير باستخدام أحد الأساليب المعتمدة في إدارة المشاريع مثل PMBOK الخاص بمعهد إدارة المشاريع أو برنس 2 PRINCE2، وهو أيضاً أسلوب آخر هام جداً سنتحدث عنه في الأقسام اللاحقة.

معايير الدليل المعرفي لإدارة المشاريع PMBOK:

إن البحث بواسطة شبكة الإنترنت عن موضوع إدارة المشاريع سينتج عنه آلاف المواضيع التي تتناول جميع القضايا والاختلافات المتعلقة بإدارة المشاريع. أفضل تلك المراجع أو المواضيع الموجودة هذه الأيام هي التي تستند إلى الدليل المعرفي لإدارة المشاريع PMBOK الصادر عن معهد إدارة المشاريع PMI والذي يعد تقريباً الأسلوب الفعلي والحقيقي الذي يصف جميع جوانب إدارة المشاريع. ونحن هنا بصدد تقديم نبذة عامة عن عمليات الدليل المعرفي لإدارة المشاريع PMBOK مع التركيز على أن يُعرف كيف يمكن أن يكون هذا الدليل مفيداً لتحسين وتعزيز وظائف حوكمة تقنية المعلومات للأنشطة الخاصة بإدارة المشاريع.

لقد تم تحديث معايير الدليل المعرفي لإدارة المشاريع بشكل منتظم، بحيث كانت تعتمد كل مجموعة جديدة من المواد الإرشادية على الإصدارات السابقة. تم إطلاق الإصدار الرابع للدليل المعرفي لإدارة المشاريع في عام ٢٠٠٨. والذي يُعرف إدارة المشاريع على أنها خمس مجموعات من العمليات الأساسية وتسعة مجالات معرفة، وهي تعتبر عناصر في جميع المشاريع تقريباً. ويمكن تطبيقها على المشاريع والبرامج والمحافظ وعمليات التشغيل. وقد أصبحت هذه المفاهيم بمثابة إطار عمل بالنسبة لإطلاق وتنفيذ المشاريع بفاعلية سواء كانت مشاريع تقنية معلومات أو غيرها. المجموعات الخمس من العمليات الأساسية لإدارة المشاريع وفقاً للدليل المعرفي لإدارة المشاريع PMBOK هي:

١- **البداية:** لا بد من وجود عمليات رسمية معمول بها لإطلاق أي مشروع. وتتضمن هذه العمليات وصف أهداف المشروع والميزانية المتوقعة والموافقات المناسبة. ويعد ذلك أحد المطالب الهامة لحوكمة تقنية المعلومات.

٢- **التخطيط:** كل مشروع بحاجة إلى تخطيط من حيث تقديرات الوقت والموارد المطلوبة بالإضافة إلى الروابط بين المكونات والمشاريع الأخرى التي تحتاج إلى تنسيق. عملية التخطيط للمشروع لها أهمية خاصة نظراً لأن معظم المشاريع يتم تنظيمها وبنائها خارج الحدود التنظيمية، ويشكل لها فرق عمل مكونة من موارد متعددة من الموارد البشرية التي تعمل بدوام جزئي لبناء عناصر المشاريع.

٣- **التنفيذ:** تحدد هذه المجموعة من العمليات الأساسية الخاصة بالدليل المعرفي لإدارة المشاريع النشاطات الفعلية للمشروع. أي ما الاحتياجات التي يجب الوفاء بها لتحقيق أهداف المشروع؟ من وجهة النظر الخاصة بتقنية المعلومات، فقد تمتد هذه النشاطات من البحث عن أدوات برمجية مناسبة إلى تفصيل برمجيات تتناسب مع متطلبات المستخدمين ومن ثم تنفيذ المشروع بعد إتمام عمليات اختبار الضوابط الداخلية المناسبة وتدريب المستخدمين.

٤- **التحكم:** وهو أحد المكونات الهامة في الحوكمة الشاملة لأنشطة المشروع. إذ لا بد من وجود عمليات معتمدة ومعمول بها لمراقبة إتمام العناصر الأساسية في المشروع والتي تعمل على تحديد ما إذا كانت الميزانيات والغايات قد تم تحقيقها أم لا.

٥- **الإغلاق:** تتطلب العملية الأخيرة إغلاق أعمال المشروع، ليأتي بعد ذلك تسليم مكونات المشروع وتلخيص نتائج المشروع وتقديم تقارير بها. وبالعودة إلى تعريفنا الرئيسي للمشروع، فإن العمل أو المسعى لا بد أن يكون له نهاية محددة يمكن أن يتم فيها تلخيص نتائج المشروع وأي خطوات تالية تم التخطيط لها للقيام بها مستقبلاً باستثناء الجهود المستقلة للمشروع.

يقوم الدليل المعرفي لإدارة المشاريع PMBOK بتوفيق أو مقابلة كل من هذه العمليات الخمس لإدارة المشاريع مع تسعة مجالات معرفة لإدارة المشاريع من حيث مدخلاتها ومخرجاتها بالإضافة إلى الأدوات والأساليب. حيث تتضمن مدخلات المشروع الوثائق والخطط والموارد اللازمة لإطلاق المشروع مع المخرجات المخطط لها، وبطبيعة الحال مواد

المشروع المكتمل. للانتقال من المدخلات الأولية للمشروع إلى المنتج النهائي الذي تم إنجازه، هناك حاجة ماسة لمجموعة واسعة من الأدوات والآليات الضرورية. فمشروع بناء منزل على سبيل المثال، سيكون بحاجة إلى خشب وخطه ولوازم أخرى كالمسامير ومواد التسقيف كمدخلات للمشروع. وتعتبر أيضاً المطرقة والمنشار ومعرفة النجارة من الأدوات الضرورية للبدء في البناء. وستكون نتيجة المشروع في هذا المثال البسيط هي المنزل الذي اكتمل بناؤه.

هناك ما هو أكثر تعقيداً بكثير من مجرد الحاجة إلى خشب أو مطرقة أو مسامير. فإطلاق العديد من مشاريع تنفيذ نظم تقنية المعلومات يتطلب تصريحاً واضحاً وصارماً بالأهداف، وخطه تفصيلية للمشروع، وخطط موارد، وخطط اختبار، والعديد من المواصفات التفصيلية الأخرى. كما يحتاج فريق تقنية المعلومات المخصص لبناء المشروع إلى فهم مجالات الاهتمام الخاصة بالمشروع؛ وأدوات كنظم الأجهزة المحمولة لتنفيذ وبناء وإطلاق عناصر ومكونات المشروع وكذلك أخصائيين على معرفة ودراية كافية في تقنية المعلومات لبناء وفحص وتنفيذ الأعمال. من عدة نواح، فإن بناء هيكل منزل يقطنه شخص يعد مشروعاً صغيراً وبسيطاً نسبياً مقارنة بالعديد من الأعمال الخاصة بالتطبيقات والبنية التحتية لتقنية المعلومات. فمعظم المشاريع التي يتم إطلاقها من قبل المؤسسات على اختلاف أنواعها تكون معقدة. وهذا التعقيد هو ما يضطرنا إلى اللجوء إلى معهد إدارة المشاريع PMI ومعايير أفضل الممارسات الموجودة في الدليل المعرفي لإدارة المشاريع PMBOK الصادر عنه. فقبل ظهور هذه المعايير، كانت المؤسسات في أغلب الأحيان تقوم بإطلاق الأعمال الرئيسية للمشروع دون أن يكون هناك تحضير واستعداد كاف. وكانت النتائج في الغالب عبارة عن تكاليف باهظة وتجاوزات في الوقت بالإضافة إلى الإخفاقات حتى في إتمام المشاريع. وقد كان لدى العديد من المشاريع التي لا علاقة لها بتقنية المعلومات المشاكل المؤسسية نفسها. فجميعها تفتقر إلى الأساليب الشاملة والمتسقة في إدارة المشاريع.

وقد عرّف الدليل المعرفي لإدارة المشاريع PMBOK عملية إدارة المشاريع على أنها عملية تحدث بطريقة متناغمة وخاضعة للرقابة على نحو جيد. وبالإضافة إلى مجموعة عمليات إدارة المشاريع الخمس الأساسية، فقد حدد الدليل المعرفي لإدارة المشاريع PMBOK تسعة مجالات معرفة خاصة بإدارة المشاريع هي:

- ١- إدارة تكامل المشروع.
- ٢- إدارة نطاق المشروع.
- ٣- إدارة وقت المشروع.
- ٤- إدارة تكلفة المشروع.
- ٥- إدارة جودة المشروع.
- ٦- إدارة الموارد البشرية للمشروع.
- ٧- إدارة اتصالات المشروع.
- ٨- إدارة مخاطر المشروع.
- ٩- إدارة مشتريات المشروع.

ويصف الدليل المعرفي لإدارة المشاريع PMBOK كلاً من هذه المجالات المعرفية التسع بتفصيل معقول ومنطقي من حيث مدخلاتها وأدواتها ومخرجاتها. على سبيل المثال، وصف مجال المعرفة الخاص بإدارة وقت المشروع في الدليل المعرفي لإدارة المشاريع PMBOK يتضمن أقساماً خاصة بالمدخلات والأدوات والمخرجات لـ:

- **تحديد أنشطة المشروع:** وهي عملية تعريف إجراءات محددة يتم تنفيذها لإنتاج الملاحق أو المخرجات الفعلية للمشروع.
- **تسلسل أنشطة المشروع الحساسة:** لا بد من تحديد وتوثيق العلاقات الموجودة بين أنشطة المشروع.
- **تقدير الموارد الخاصة بالنشاط:** يجب تقدير أنواع وإعداد الأشخاص وكميات المواد والمعدات واللوازم المطلوبة لإتمام الأنشطة المجدولة للمشروع.
- **تقدير الفترات الزمنية للنشاط:** هناك ضرورة ملحة لتحليل تسلسل أنشطة المشروع والفترات الزمنية ومتطلبات موارد ووقت واحتياجات موارد المشروع، وذلك لجدولة أعمال ونشاطات المشروع.

• وضع الجدول الزمني للمشروع: إن خطة متابعة التقدم الذي يتم إحرازه تكون ضرورية لمراقبة حالة المشاريع لتحديث الإنجازات الخاصة بها وإدارة أي تغيرات قد تطرأ على الجداول الزمنية الخاصة بها.

هذه هي الخطوات الأساسية لإدارة الوقت بالنسبة لأي مشروع، وهي تعد بالتأكيد الأنشطة الرئيسية التي ينبغي على وحدة تقنية المعلومات في المؤسسة أخذها بعين الاعتبار عند قيامها بالتخطيط لمتطلبات الوقت لأي مشروع من مشاريع تقنية المعلومات.

بالإضافة للدليل الخاص بالإدارة العامة، فإن الدليل المعرفي لإدارة المشاريع (PMBOK) يحدد بشكل تفصيلي أدوات إدارة المشاريع وعملياتها اللازمة في كل مجال من مجالات المعرفة التي أشرنا إليها. يلخص الشكل التوضيحي (١٦-٢) هذه العمليات وكذلك مجالات المعرفة الخاصة بالدليل المعرفي لإدارة المشاريع PMBOK. لا يهدف هذا الفصل إلى تقديم نظرة تفصيلية عن جميع عمليات ومجالات المعرفة الخاصة بالدليل المعرفي لإدارة المشاريع PMBOK، إنما يهدف إلى التركيز على الدور الذي يلعبه الدليل المعرفي لإدارة المشاريع PMBOK في التخطيط والتنفيذ للعمليات الفعالة الخاصة بإدارة مشاريع تقنية المعلومات. إذ تستند الأرقام المرجعية في الشكل التوضيحي (١٦-٢) إلى مواد الدليل المعرفي لإدارة المشاريع PMBOK، ولكن ما يهم هنا هو أن هذه الأرقام تؤكد الخطوات اللازمة لبناء مشاريع فعالة. على سبيل المثال، مجال المعرفة رقم ٧ عبارة عن إدارة تكلفة المشروع، وهي خطوات ضرورية لأي عملية من عمليات المشروع ويوضح الشكل التوضيحي (١٦-٢) مجموعات العمليات الضرورية، وهي تقدير التكاليف وبناء الميزانية والتحكم في هذه التكاليف.

أسلوب آخر لإدارة المشاريع: برنس ٢ Prince2:

برنس ٢ PRINCE2 هو أحد الأساليب الأخرى لإدارة المشاريع والمُعترف بها بشكل قوي. وهو أسلوب معتمد على العمليات ومرتبطة أكثر بالمواد الإرشادية الخاصة بإطار العمل آيتل الذي تحدثنا عنه في الفصل السادس من هذا الكتاب. وقد تم إطلاق الإصدار الأول من معيار PRINCE2 في عام ١٩٩٦ باعتباره طريقة أو منهجية عامة لإدارة المشاريع. وعلى الرغم من أنه لا يزال حتى الآن غير شائع الاستخدام في الولايات المتحدة، فإن أسلوب

PRINCE2 أصبح مألوفاً على نحو متزايد بل ويعد هذه الأيام بمثابة الأسلوب الفعلي لإدارة المشاريع في كل من المملكة المتحدة ودول الاتحاد الأوروبي. إن PRINCE2 عبارة عن أسلوب معياري لإدارة المشاريع يعتمد على العمليات فهو قائم على مجموعة من المبادئ والعمليات المحددة لإدارة المشاريع. يصف الشكل التوضيحي (١٦-٣) عملية إدارة المشاريع وفقاً لمنهجية PRINCE2.

ومقارنة بالدليل المعرفي لإدارة المشاريع PMBOK، فإن منهجية PRINCE2 تعد أكثر توجهاً واعتماداً على حالة الأعمال من الدليل المعرفي لإدارة المشاريع PMBOK. ومن خلال هذه المنهجية أيضاً فإن إدارة المشاريع تكون موجهة نحو قيام الإدارة العليا بها أكثر من أن يقوم بها فريق العمل المباشر. وتعد هذه المنهجية في كثير من النواحي أحد أفضل أدوات حوكمة تقنية المعلومات فيما يتعلق بإدارة المشاريع والإشراف عليها. ومع ذلك، فإننا لا نهدف من خلال هذا الفصل إلى وصف كيفية تطبيق منهجية برنس ٢ PRINCE2 لإدارة المشاريع، ولكننا نهدف فقط إلى تسليط الضوء عليه باعتباره أداة بديلة عن الدليل المعرفي لإدارة المشاريع PMBOK للقيام بإدارة وضبط مشاريع تقنية المعلومات. وينبغي على فريق الإدارة الذي يساعد في وضع ومراجعة ضوابط حوكمة تقنية المعلومات الخاصة بإدارة المشاريع أن يُصر على ضرورة اتباع إدارة تقنية المعلومات لهذه المنهجيات الموضوعة فيما يتعلق بالتخطيط والإشراف على أنشطة المشاريع الخاصة بها. قد يستخدم العديد في هذه الأيام الدليل المعرفي لإدارة المشاريع PMBOK والذي يتسق مع الإدارة الفعالة لحوكمة تقنية المعلومات. على كل حال، إذا كانت إدارة تقنية المعلومات لم تقم بعد باعتماد الدليل المعرفي لإدارة المشاريع PMBOK، فإن على الإدارة الأخذ بالنصيحة التي تحث على تبني وحدة تقنية المعلومات لمعايير PRINCE2 نظراً لأنها تتوافق بشكل كبير مع أفضل ممارسات إطار العمل آيتل التي تناولناها في الفصل السادس من هذا الكتاب.

محفظة نظم تقنية المعلومات وإدارة البرامج:

يقوم مديرو المشاريع غالباً باستخدام مصطلح "برنامج" عندما يتحدثون عن عدة مشاريع. يكون البرنامج في العادة عبارة عن مشروع رفيع المستوى يُستخدم لإدارة سلسلة من المشاريع المترابطة والمتصلة بعضها ببعض. على سبيل المثال، قد ترغب المؤسسة في

تنفيذ مبادرة كبيرة إلى حد ما، فيتم تقسيمها إلى سلسلة من المشاريع المنفصلة. ويستطيع كل مشروع من هذه المشاريع العمل بشكل مستقل، غير أن هيكل البرنامج يقوم بإدارة جميع هذه المشاريع معاً. ويستخدم هذا الفصل عموماً مصطلح "مشروع" للدلالة على عمل أو جهد فردي، ومصطلح "برنامج" للدلالة على عدة مشاريع مترابطة فيما بينها. وهناك مصطلح آخر ألا وهو محفظة استثمارات تقنية المعلومات Portfolio of IT Investments، والذي يشير عادة إلى المكان أو المستودع الخاص باستثمارات المشاريع القائمة. فعادة ما يتم تجميع عدة مشاريع مترابطة بعضها مع بعض في برامج ومحافظ مشاريع.

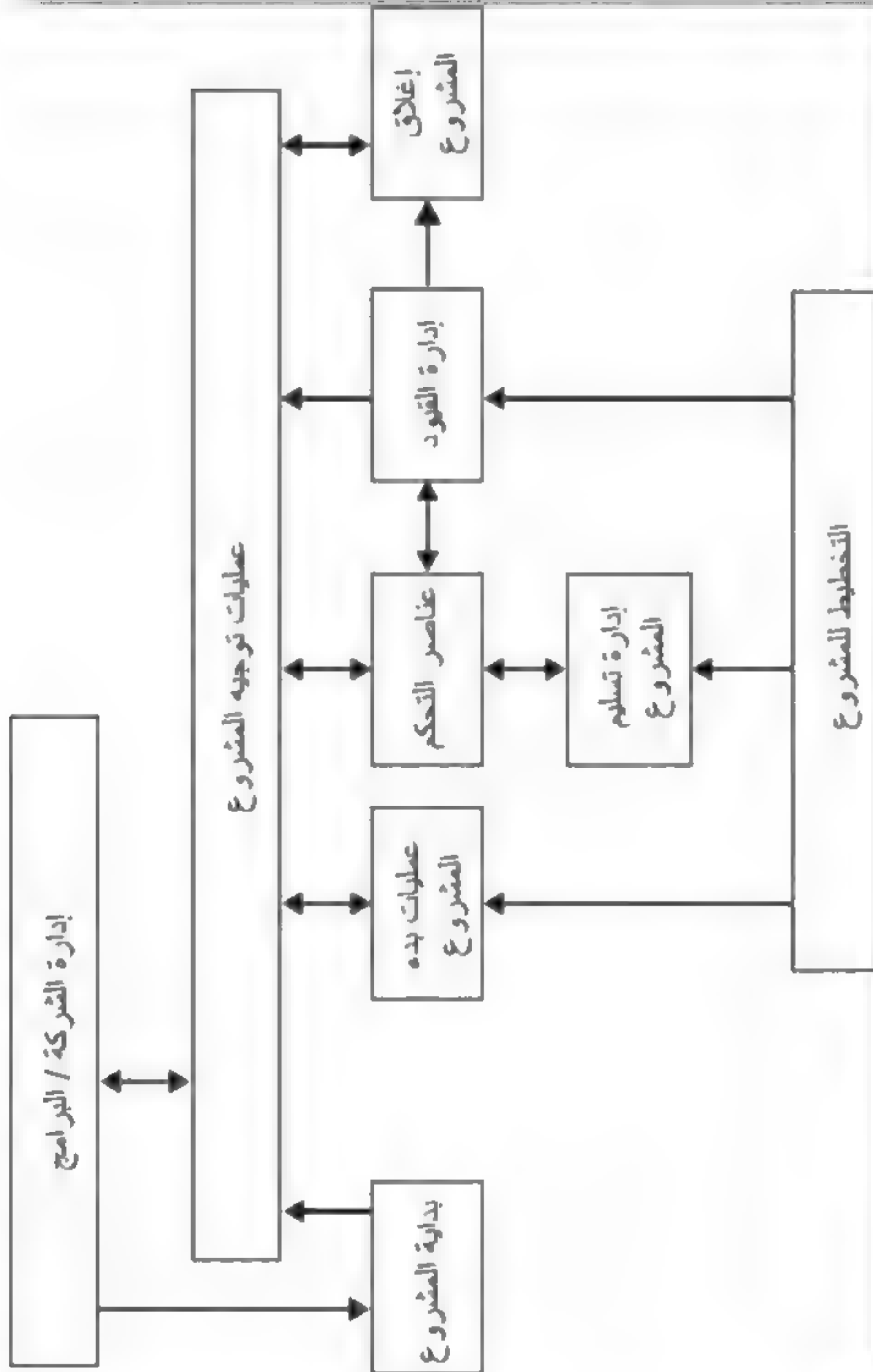
الشكل (١٦-٢)

موجز مجموعات العمليات ومجالات المعرفة الخاصة بالدليل المعرفي لإدارة المشاريع PMBOK

مجال المعرفة	مجموعات عمليات إدارة المشاريع				
	مجموعة عمليات البدء	مجموعة عمليات التخطيط	مجموعة عمليات التنفيذ	مجموعة عمليات المراقبة والتحكم	مجموعة عمليات الإغلاق
٤ إدارة تكامل المشروع	١-٤ وضع ميثاق المشروع	١-٤ وضع خطة إدارة المشروع ٢-٤ وضع خطة إدارة ٣-٤ وضع مخطط تنجز WBS	٣-٤ توجيه وإدارة تنفيذ المشروع	٤-٤ مراقبة صلب المشروع ٥-٤ تنفيذ الرقابة المتكاملة للتغيرات	٦-٤ إغلاق المشروع أو المرحلة
٥ إدارة نطاق المشروع		١-٥ جمع المتطلبات ٢-٥ تحديد النطاق ٣-٥ وضع مخطط تنجز WBS		٤-٥ التحقق من النطاق ٥-٥ ضبط النطاق	
٦ إدارة وقت المشروع		١-٦ تحديد الأنشطة ٢-٦ تقدير الموارد ٣-٦ تقدير موارد النشاط ٤-٦ تقدير الفترات الزمنية ٥-٦ وضع الجدول الزمني		٦-٦ ضبط الجدول الزمني	
٧ إدارة تكلفة المشروع		١-٧ تقدير التكاليف ٢-٧ تحديد السعر البنية		٣-٧ ضبط التكاليف	
٨ إدارة جودة المشروع		١-٨ وضع خطة جودة	٢-٨ تطبيق ضمان الجودة	٣-٨ نفذ مراقبة الجودة	
٩ إدارة الموارد البشرية للمشروع		١-٩ وضع خطة الموارد البشرية	٢-٩ الحصول على فريق المشروع ٣-٩ تطوير فريق المشروع ٤-٩ إدارة فريق المشروع		
١٠ إدارة اتصالات المشروع		١-١٠ وضع خطة الاتصالات	٢-١٠ توزيع المعلومات ٣-١٠ إدارة توافقات المستفيدين	٥-١٠ إعداد تقرير الأداء	
١١ إدارة مخاطر المشروع		١-١١ وضع خطة إدارة المخاطر ٢-١١ تحديد المخاطر ٣-١١ إجراء التحليل الكمي للمخاطر ٤-١١ التحليل النوعي للمخاطر		٦-١١ المراقبة والتحكم بالمخاطر	
١٢ إدارة مشتريات المشروع		١-١٢ وضع خطة مشتريات	٢-١٢ متطلبات السلوك	٣-١٢ إدارة المشتريات	٤-١٢ إغلاق المشتريات

شكل توضيحي (٣-١٦)

عملية إدارة المشاريع وفقاً لمنهجية PRINCE2



يتكون برنامج إدارة المشاريع من سلسلة من المشاريع المترابطة التي تدار بطريقة متناسقة للحصول على المزايا والضوابط التي لا يمكن أن تكون متاحة في حال كانت هذه المشاريع تدار بشكل مستقل ومنفصلة بعضها عن بعض. حيث تتكون البرامج بشكل عام من عمل مترابط قد يكون خارج نطاق المشاريع المنفردة.

تظهر الحاجة إلى إدارة البرنامج بشكل عام عندما يكون لدى المؤسسة هدف فردي محدد يمكن تحقيقه من خلال سلسلة من المشاريع المنفصلة. على سبيل المثال، خطة نقل منشأة صناعية إلى موقع جديد، تتطلب وجود سلسلة من المشاريع المنفصلة التي بحاجة إلى تنسيق. قد يتطلب أحد المشاريع هنا نقل وتركيب معدات الإنتاج، وقد يتطلب الآخر نقل المواد الخام، وسيبقى هناك مشروع آخر منفصل سيعمل على تغطية موضوع تحويلات نظم تقنية المعلومات. وعلى الرغم من أنه يجب أن يكون هناك شخص ما يكون مسؤولاً عن تنسيق جميع هذه الأعمال، فإن كل مشروع سيكون له احتياجاته ومتطلباته الخاصة. حيث سيتم إدارة هذه المشاريع بشكل منفصل ولكن بعد تجميعهم معاً كبرنامج واحد.

ينبغي على حوكمة تقنية المعلومات النظر إلى متطلبات المشاريع المترابطة والخاصة بتدقيق تقنية المعلومات على أنها برنامج. على سبيل المثال، قد يُطلب من المؤسسة مراجعة الضوابط الداخلية في مجموعة من المنشآت وفقاً لقانون SOX البند ٤٠٤. حتى وإن كان كل مشروع من هذه المشاريع المستقلة سيتم تنفيذه على أنواع مختلفة من المرافق وفي مناطق جغرافية مختلفة وتحت مسؤولية فرق مختلفة في إدارة تقنية المعلومات؛ فإن كل مشروع من هذه المشاريع سيكون له الأهداف العالية المستوى نفسها، وقد يكون أحد كبار المديرين هو المسئول عن إتمام كل واحد من هذه المشاريع بشكل كلي. حيث يمكن تنظيم وإدارة هذه المجموعات من المشاريع في برنامج، مع قيام كل مدير من مديري المشاريع المستقلة بإعداد وإرسال التقارير إلى مدير البرنامج من أجل تحقيق الامتثال العام لكامل العمل.

وبالانتقال من مستوى إلى آخر أعلى، حيث مصطلح إدارة المحافظ الذي يشير إلى مجموعات من المشاريع والبرامج والأعمال الأخرى التي يتم تجميعها معاً لتسهيل إدارتها على نحو فعال. في حال وجود مجموعات مستقلة لتقنية المعلومات في إدارتين داخل إحدى

الشركات، وربما تكون واحدة من هذه المجموعات مسؤولة عن العمليات التشغيلية للبنية التحتية لتقنية المعلومات في دول الاتحاد الأوروبي، في حين أن الأخرى مسؤولة عن ذلك في الولايات المتحدة الأمريكية وكندا. في هذه الحالة يمكن اعتبار الأنشطة الشاملة لتقنية المعلومات لكل وحدة من الوحدات عبارة عن حافظة (محفظة) لإدارة تقنية المعلومات، حيث يمكن إدراج كلٍّ منهما تحت محفظة ذات مستوى أعلى في المقر الرئيسي للشركة. إن هذه المفاهيم التي تتعلق بإدارة كل من المشاريع والبرامج والمحافظ موضحة بالشكل التوضيحي (٤-١٦). الفكرة هي أن تلك العلاقات الواردة بالشكل يجب إنشاؤها إذا اقتضت الحاجة وذلك لتعزيز الكفاءة وتحقيق الأهداف العامة.

شكل توضيحي (٤-١٦)

نظرة عامة على إدارة المشاريع والبرامج والمحافظ.

المحافظ	البرامج	المشاريع	
المحافظ لها نطاق أعمال يتغير بتغير الأهداف الإستراتيجية للمؤسسة.	البرامج لها نطاقات أكبر وتقدم مزايا أعظم.	المشاريع لها أهداف محددة. سيتضح النطاق تدريجياً خلال دورة حياة المشروع.	النطاق
يراقب مديرو المحافظ باستمرار التغيرات في البيئة الواسعة.	يجب على مديري البرامج أن يتوقعوا التغير سواء من داخل أو خارج البرنامج وأن يعدوا لإدارته.	يتوقع مديرو المشاريع التغير ولذا يقومون بتنفيذ عمليات لإدارة التغير والتحكم فيه.	التغيير
يقوم مديرو المحافظ بإنشاء العمليات والاتصالات الضرورية ذات الصلة بالمحفظة الإجمالية والإبقاء عليها.	يضع مديرو البرامج الخطة الشاملة للبرنامج ويضعون خططاً عالية المستوى لتوجيه التخطيط التفصيلي على مستوى العنصر.	مديرو المشاريع بحاجة إلى التخطيط للتطور التدريجي من تخطيط عالي المستوى إلى تخطيط تفصيلي خلال دورة حياة المشروع.	التخطيط
قد يدير مديرو المحافظ وينسقون أعضاء فريق إدارة المحفظة.	يدير مديرو البرامج أعضاء فريق البرنامج ومديري المشاريع. فهم يقدمون الرؤية وتكون لهم ملكية البرنامج بالكامل	يدير مديرو المشاريع فريق المشروع لتحقيق أهداف المشروع.	الإدارة

النجاح	يقاس النجاح بجودة المنتج والمشروع وبالفترات الزمنية والالتزام بالميزانية ومستوى رضا العملاء.	يقاس النجاح بالدرجة التي عندها يتم تحقيق البرنامج للاحتياجات والمزايا التي من أجلها تم وضع البرنامج.	يقاس النجاح من حيث الأداء الكلي التجميعي لمكونات المحفظة.
الرقابة	يقوم مديرو المشاريع بمراقبة وضبط عمليات تقديم المنتجات والخدمات والنتائج التي أقر المشروع من أجلها.	يراقب مديرو البرنامج التقدم التدريجي لمكونات البرنامج لضمان الالتزام بكل من الأهداف العامة والجداول الزمنية والميزانية وتحقيق المزايا المرجوة.	يراقب مديرو المحافظ مؤشرات الأداء والقيمة التجميعية.

بالإضافة إلى مراجعة وإدارة المشاريع والمحافظ الفردية لتقنية المعلومات، فإن الدليل الموضح في الشكل التوضيحي (١٦-٤) مفيد لإدارة تقنية المعلومات، حيث يوجد عدة مشاريع متشابهة لتدقيق تقنية المعلومات، والتي يمكن إدارتها كبرنامج أو اعتبارها جزءاً من محفظة مشاريع. الفكرة العامة هي أنه لا بد من أن يكون هناك تفاعل قوي بين البرامج أو المحافظ ومشاريعهم المستقلة أو التابعة، غير أن إدارة البرنامج لا تستطيع في الغالب أن توجه أو تملّي شروطها على أنشطة المشاريع الفردية، كما أن المشاريع الفردية سوف تساعد في تحديد البنية العامة للبرامج الداعمة. فالتشابه بين سلسلة عمليات التدقيق المستقلة لتقنية المعلومات وبين الإدارة العامة للتدقيق يكون قوياً للغاية.

إن العديد من إدارات تقنية المعلومات هذه الأيام محمّلة بالعديد من البرامج والمشاريع. حيث نجد أن بعض هذه المبادرات منظم على نحو جيد في حين يفتقر البعض الآخر للترابط الجيد حتى إنها تبدو عشوائية. وكأحد العناصر الهامة في حوكمة تقنية المعلومات، يجب أن يكون هناك أعمال ومجهودات جارية ومستمرة لجعل إدارة تلك المبادرات الإستراتيجية الخاصة بالمشاريع أبسط وأكثر فاعلية. أما فيما يخص الحلول التي تقدمها حوكمة تقنية المعلومات في هذا الصدد فهو بناء أساس قوي لإدارة محافظ المشاريع. إن إدارة احتياجات المشاريع ومواردها وميزانياتها على نحو فعال تعد بمثابة المفتاح الرئيسي لتقديم مبادرات تتعلق بحوكمة تقنية معلومات والتي تعمل على قيادة الشركة إلى الأمام وتصبح المسار الصحيح الذي يساعد المؤسسة على تحقيق أهدافها.

مكتب إدارة البرامج (PMO)، أحد الموارد القوية للحوكمة:

كما تحدثنا سابقاً، فإن البرنامج عبارة عن مشروع ذي مستوى أعلى يعمل ليكون أداة للإدارة والإشراف على مشاريع أخرى، وهي المشاريع الفرعية. وقد بدأ ظهور هذا المفهوم في مجال تقنية المعلومات خلال سنوات استهلكت فيها أقسام تقنية المعلومات طاقاتها من أجل تسليم مشاريع مطلوبة في الوقت المحدد وفي حدود الميزانيات المخصصة. وقد كان الحل هو ضبط المشاريع بإحكام من خلال تأسيس ما يعرف بمكاتب إدارة البرامج (PMO) Program Management Offices باعتبارها وسيلة لتعزيز كفاءة تقنية المعلومات وخفض التكاليف وتحسين أداء المشاريع من حيث الالتزام بالوقت والميزانية. فما تم فعله لمشاريع تقنية المعلومات يمكن عمله تماماً على نحو جيد للمشاريع الأخرى في المؤسسة.

قد يقدم مكتب إدارة البرامج PMO المعايير أو سلطة الموافقة على جميع المشاريع أو حتى مهارات إدارة المشاريع وذلك من خلال كادر مكون من مجموعة من المحترفين المعتمدين في إدارة المشاريع. حيث تستطيع الوحدة الخاصة بمكتب إدارة البرامج PMO غرس الانضباط في إدارة المشاريع الذي تشتد الحاجة إليه في أقسام تقنية المعلومات وجميع المجموعات الأخرى المشاركة في إدارة المشاريع. كما يمكن لمكتب إدارة البرامج PMO المساعدة من خلال تقديم البنية اللازمة لتوحيد ممارسات إدارة المشاريع وتسهيل إدارة محافظ المشاريع بالإضافة إلى تحديد منهجيات لعمليات متكررة. ويعد قانون SOX - الذي يطالب الشركات بالإفصاح عن الاستثمارات، كالمشاريع الضخمة، التي قد تؤثر في الأداء التشغيلي للشركة - أحد العوامل المحفزة في هذا الصدد، فقد أجبر الشركات على عمل مراقبة حثيثة على نفقات المشروع ومدى تقدمه.

هناك نموذجان أساسيان لمكاتب إدارة البرامج PMOs: أحدهما يعمل بصفة استشارية حيث يزود مديري المشاريع في وحدات الأعمال بالتدريبات والإرشادات، وأفضل الممارسات. أما النموذج الآخر فيعمل على أنه مركز به مجموعة من مديري المشاريع يتم إعارتهم إلى وحدات الأعمال للعمل بصفة مديري مشاريع. إن الكيفية التي يتم بها تنظيم وإدارة مكتب إدارة البرامج (PMO) وتعيين الكوادر المؤهلة للعمل فيه تعتمد على عدد كبير من العوامل التنظيمية، من ذلك الغايات المستهدفة، ونقاط القوة التقليدية، والدوافع

الثقافية. فبتبني فكرة وجود مكتب لإدارة البرامج (PMO) بما يتماشى مع ثقافة إدارة تقنية المعلومات، يمكن لمكتب إدارة البرامج PMO أن يساعد المؤسسة في القيام بالمشاريع الإستراتيجية التي تُرضي كلاً من المستخدمين الداخليين والخارجيين. ومع مرور الوقت، يجب أن يكون مكتب إدارة البرامج PMO قادراً على تزويد المؤسسة بالفوائد المالية من خلال تفعيل إدارة أفضل للموارد وتقليص فشل المشاريع ودعم تلك المشاريع التي تعود على المؤسسة بفائدة أكبر.

تكون مكاتب إدارة البرامج PMOs عادة عبارة عن وحدات إدارية لدعم إدارة تقنية المعلومات، وقد تختلف هذه المكاتب من حيث أحجامها وبنيتها ومسؤولياتها. فهي تقدم إرشادات في إدارة المشاريع لمديري المشاريع في وحدات الأعمال وتعمل غالباً في مجالات الدعم التالية:

- **عملية / منهجية لإدارة المشاريع:** سواء كانت وحدة تقنية المعلومات في المؤسسة تستخدم الدليل المعرفي لإدارة المشاريع PMBOK أو برنس 2 PRINCE2، فبإمكان مكتب إدارة البرامج PMO أن يقدم الإرشادات لتطوير وتنفيذ عمليات متناغمة وقياسية لإدارة المشاريع.
- **التدريب على إدارة المشاريع:** وتعتبر هذه النقطة من المجالات الفعالة، حيث بإمكان مكتب إدارة البرامج PMO أن يقوم بعقد برامج تدريبية تتعلق بالمشاريع أو جمع متطلبات التدريب لكي تقوم بها شركة تدريب خارجية.
- **مقر لمديري المشاريع:** بما أن مكتب إدارة البرامج PMO يعتبر بمثابة مصدر مركزي للمعرفة والدعم اللازمين لإدارة المشاريع، فبإمكانه الإبقاء على مكتب مركزي حيث يتم منه إعارة مديري المشاريع للخارج عند انتهاء المشروع المعين عليه.
- **الاستشارات والتوجيهات الداخلية:** بهدف تشجيع التميز في إدارة المشاريع، يستطيع مكتب إدارة البرامج PMO أن يقدم النصائح للموظفين الآخرين فيما يتعلق بأفضل الممارسات مع التركيز على الدليل المعرفي لإدارة المشاريع PMBOK.
- **الأدوات البرمجية لإدارة المشاريع:** يمكن اختيار الأدوات البرمجية المخصصة لإدارة المشاريع وصيانتها لكي تستخدم من قبل جميع المشاركين في المشاريع، حيث يوجد العديد من المواد

البرمجية المتاحة لدعم أنشطة إدارة المشاريع. كما يمكن أن يعمل مكتب إدارة البرامج PMO بمثابة مركز لتبادل المعلومات فيما يتعلق باستخدام تلك الأدوات البرمجية.

• **إدارة المحفظة:** وضع فريق مكون من مديري المشاريع قادر على إدارة عدة مشاريع مترابطة مثل المشاريع الخاصة بتقنيات البنية التحتية، ومشاريع التطبيقات المكتبية وغيرها من المشاريع، وتخصيص الموارد وفقاً لذلك.

ربما توجد أساليب مختلفة لدى المنظمة للقيام بإدارة الوحدة الخاصة بمكتب إدارة البرامج PMO. لكن الطريقة المركزية التي تمتاز بالممارسة العملية على التحكم في المشاريع تكون غالباً أكثر فاعلية في المنظمات التي يتعامل فيها مكتب إدارة البرامج PMO بشكل نظامي مع كبار المديرين التنفيذيين ولديه كامل الصلاحية بإلغاء مشاريع أو وضع أولويات لها. فمن خلال استخدام منهجيات واضحة المعالم لإدارة المشاريع، فإن مكتب إدارة البرامج يمكنه غالباً العمل مع وحدات الأعمال في كل جانب من جوانب إدارة المشاريع ابتداءً من تحديد المتطلبات الرئيسية إلى المرحلة الخاصة بإجراء عمليات التدقيق التي تلي عملية التنفيذ. إن الإبقاء على عمليات متناغمة عبر المنظمة من شأنه أن يمكن المنظمة من القيام بتجزئة المشاريع إلى مكونات أصغر يمكن إدارتها ومن ثم التقليل من الفشل.

تمتد مسؤوليات مكاتب إدارة البرامج PMOs بشكل واسع من توفير مركز لتبادل المعلومات المتعلقة بأفضل ممارسات إدارة المشاريع إلى إجراء المراجعات الرسمية لإدارة المحافظ. وليس من الضروري أن يقتصر إشراف مكتب إدارة البرامج فقط على تطوير المشاريع بل قد تشمل التنسيق وتتبع كلاً من المشاريع والخدمات. لذا يعد إنشاء مكتب لإدارة البرامج PMO للعمل في أي منظمة بمثابة تدريب على التكيف وقوة التحمل. فعندما يتعلق الأمر بإنشاء مكتب لإدارة البرامج PMO، فإن هناك عدداً محدوداً من خرائط الطرق التي يمكن اتباعها، أو المعايير القياسية التي يسارع بتبنيها، أو المقاييس التي يمكن القياس على أساسها. إن أكثر مكاتب إدارة البرامج PMOs فاعلية هي تلك التي تجني التحسينات مع مرور الوقت وتدفع المنظمة دائماً إلى تحسين أدائها.

إدارة المشاريع ومكتب إدارة البرامج (PMO) وحوكمة تقنية المعلومات:

تقوم المؤسسات ببناء وتأسيس مبادرات تقنية المعلومات وغيرها من المبادرات الرئيسية الخاصة بها من خلال المشاريع. وكما ذكرنا، فإن المشاريع وإدارة المشاريع الخاصة بتقنية المعلومات تعمل غالباً خارج الحدود التنظيمية للمنظمة. فمبادرة تنفيذ نظام جديد لحساب تكاليف الإنتاج مثلاً، قد تحتاج إلى موارد من نظم وبرامج تقنية المعلومات، بالإضافة لأشخاص من إدارة الحسابات ووحدات الإنتاج المختلفة. فعندما تكون هذه الجهود خاضعة لإشراف مدير المشروع المعين، يمكن الحصول على الموارد واتخاذ الخطوات اللازمة لتنفيذ نظام حساب تكاليف الإنتاج المطلوب.

إن الاستخدام الفعال لمبادئ إدارة المشاريع يعد أحد العناصر الهامة في الحوكمة الفعالة لتقنية المعلومات. لذا يجب على إدارة تقنية المعلومات أن تتبنى منهجية لإدارة المشاريع مثل الدليل المعرفي لإدارة المشاريع PMBOK مثلاً. والأهم من ذلك، هو وجود ما يثبت أن جميع المشاريع القائمة حالياً تستخدم هذا الأسلوب، وأنها تمتلك أساليب فعالة معمولاً بها في تخطيط المشاريع، هذا بالإضافة إلى وجود مثل تلك الوثائق التي يعلن فيها صراحة عن أهداف المشروع وخطط ضمان الجودة الموضوعية موضع التنفيذ. كما يجب أن يكون هناك دليل على وجود عمليات منهجية معمول بها لإدارة مشاريع تقنية المعلومات.

إذا كانت إدارة تقنية المعلومات تقوم باستخدام عمليات المشروع لبناء وإدارة العديد من أنشطته، وإذا كان هناك عدد كبير من المشاريع المترابطة، فعلى إدارة تقنية المعلومات أن تقوم بتأسيس مجموعة فعالة من العمليات الخاصة بمكتب إدارة البرامج PMOs. حيث تعد عملية إدارة البرامج أحد العمليات الهامة متى كان هناك عدد كبير من عمليات المشاريع المستخدمة في بناء وتنفيذ مشاريع وعمليات تقنية المعلومات. إن العمليات الفعالة في إدارة مشاريع تقنية المعلومات سوف تسهم في تحسين العمليات الشاملة في حوكمة تقنية المعلومات.

ملاحظة:

1- Project Management Institute, A Guide to the Project Management Book of Knowledge (PMBOK Guide), 4th ed. (Newtown Square, PA: 2008).

الفصل السابع عشر

اتفاقيات مستوى الخدمات (SLAs) ومنتدى إدارة خدمات تقنية المعلومات (itSMF) وقيمة تقنية المعلومات (Val IT) وتعظيم استثمارات تقنية المعلومات

منذ سنوات عديدة، تم تركيب نظم الحاسبات المركزية الأولى Mainframe في معظم الشركات الكبيرة. وكان ذلك بهدف تسير العمليات التشغيلية والتقليل من التكاليف، وقد كان أحياناً بهدف إعطاء السمعة أو المكانة للشركات. وقد كان ذلك في الأيام الأولى عندما كانت تلك النظم المركزية الباهظة الثمن توضع في أغلب الأحيان في غرف زجاجية محكمة الإغلاق في أروقة داخل الشركات، وكان هناك توقعات كبيرة حول الفوائد التي ستعود على الأعمال جراء هذه التقنية الجديدة. لكن سرعان ما تبعها خيبة أمل كبيرة. ونظراً للمخاوف المتعلقة بموضوع الأمان والمساحة، فسرعان ما تم نقل تلك الأجهزة المركزية ومجموعة محركات الأشرطة والوحدات التخزينية المتزايدة الخاصة بها إلى مواقع بعيدة تابعة للشركة. والأهم من ذلك، كانت المدخرات الاستثمارية العائدة بطيئة نظراً للتكلفة الخاصة بتوظيف وبناء كادر من المتخصصين العاملين في تقنية المعلومات، وكذلك بسبب حالات التأخير والتكاليف المصاحبة للعديد من مشروعات تطوير تقنية المعلومات، وأيضاً بسبب البرامج التطبيقية التي لم تكن تعمل بالشكل الجيد كما هو متوقع. وسرعان ما أدركت المؤسسات أن هناك حاجة ماسة لمراجعة استثماراتها في مجال تقنية المعلومات الخاصة بها على جميع المستويات ومحاولة تحقيق المزيد من الفوائد الناتجة عنها.

يستعرض هذا الفصل القضايا والمخاوف المتعلقة بحوكمة تقنية المعلومات من عدة جهات نظر فيما يتعلق باستثمارات المؤسسة في موارد تقنية المعلومات. وسوف نبدأ الحديث أولاً عن أهمية وضع اتفاقيات مستوى الخدمات SLAs وإدارتها على نحو فعال على أنها جزء من عمليات تشغيل تقنية المعلومات الخاصة بالمؤسسة. حيث تعد اتفاقيات مستوى الخدمة SLAs والإرشادات الخاصة بإدارة الخدمات المرتبط بها واحدة من أفضل الممارسات الخاصة

بإطار العمل آيتل التي تم تقديمها للمرة الأولى في الفصل السادس من هذا الكتاب. وهي عبارة عن مجموعة من التفاهات أو العقود الداخلية بين مستخدمي خدمات تقنية المعلومات وإدارة تقنية المعلومات. فهي تصف الخدمات التي ستقدمها وحدة تقنية المعلومات للإدارات المختلفة للمستخدمين وتشمل الملفات والتقارير المحدثة، إضافة إلى تسليم الملفات والوثائق المحددة في الوقت المناسب. كما سنؤكد أهمية اتفاقيات مستوى الخدمة SLAs على أنها إحدى الأدوات الهامة لحوكمة تقنية المعلومات وسنتحدث أيضاً عن كيفية تطبيق هذه الاتفاقيات في المؤسسة وحصد المزايا والفوائد الناتجة عنها على نحو أكثر فاعلية.

المنتدى الذي يمكن اعتباره مرتبطاً ارتباطاً وثيقاً بإطار العمل آيتل لكنه مستقل عنه، هو منتدى إدارة خدمات تقنية المعلومات (IT Service Management Forum (itSMF. وهو عبارة عن منظمة ذات عضوية مهنية مستقلة قامت بتعزيز وترويج العمليات الخاصة بإدارة خدمات تقنية المعلومات ونشرت بعض الإرشادات التي لها علاقة بهذه المجالات. فمن خلال الفروع المحلية في العديد من المدن الرئيسية ومع الاهتمام القوي والمتزايد بقضايا حوكمة تقنية المعلومات. فإن منتدى إدارة خدمات تقنية المعلومات itSMF هو المنظمة التي ربما يهتم بها محترفو الإدارة لمزيد من البحث والاستكشاف. سيقدم هذا الفصل هذه المجموعة الاحترافية ويسلط الضوء على بعض نقاط القوة المتعلقة بحوكمة تقنية المعلومات الخاصة بها.

سيقدم هذا الفصل أيضاً بشكل موجز ما يُعرف بالمجموعة المفتوحة للامتثال والأخلاقيات (Open Compliance and Ethics Group (OCEG ومعايير الحوكمة وإدارة المخاطر والامتثال GRC الخاصة بها.

كما سيقدم هذا الفصل أيضاً بعض التفاصيل الإضافية عن معايير الحوكمة الخاصة بهذه المجموعة مع التركيز على "الكتاب الأحمر" الخاص بهذه المجموعة. ومن المؤكد أننا سنلاحظ التركيز المتزايد على المعايير الخاصة بالمجموعة المفتوحة للامتثال والأخلاقيات OCEG باعتبارها أدوات تستخدم لتحسين حوكمة تقنية المعلومات في السنوات القادمة. وسناقش هذا الفصل بعض المعايير والأدوات التي صدرت عن منتدى إدارة خدمات تقنية المعلومات لتحسين كل من حوكمة تقنية المعلومات ومخاطر الأعمال والاحتيايل.

قامت جمعية تدقيق وضبط نظم المعلومات (ISACA) التي تم تقديمها في فصول سابقة بتطوير وإصدار مجموعة من المواد الإرشادية التي أطلق عليها مصطلح قيمة تقنية المعلومات Val IT التي تهدف إلى فهم وتقييم الاستثمارات التي خصصتها المؤسسة لموارد تقنية المعلومات لديها على نحو أفضل. كما سيقوم هذا الفصل بتقديم نموذج قيمة تقنية المعلومات Val IT وسيوضح لماذا يعد هذا النموذج واحداً من المفاهيم الهامة التي من الممكن أن تساعد الإدارة العامة وإدارات تقنية المعلومات التابعة لها في العمل سوياً على نحو أفضل بهدف تحقيق قيمة أكبر من عمليات تقنية المعلومات الخاصة بهم.

سيُختتم هذا الفصل ببعض الإرشادات العامة بالنسبة للمؤسسة فيما يتعلق بقياس وتحقيق القيمة المكتسبة من استثمارات تقنية المعلومات الخاصة بها. إننا مع مرور الوقت أصبحنا أكثر ذكاءً، وذلك عندما تلاشت بشكل كبير نظم الحاسبات المركزية الضخمة والمكلفة. وأصبحنا الآن نقوم وفي فترات زمنية صغيرة بتجميع التطبيقات الجديدة من قائمة الخيارات الموجودة في نظام قائم على السحابة بدلاً من بناء تلك التطبيقات داخلياً من قبل طاقم التطوير الموجود في المؤسسة. ومع ذلك فإن المؤسسة بحاجة إلى معرفة تكاليف تلك النظم واتخاذ التدابير والإجراءات المناسبة لتحقيق أكبر قيمة ممكنة. ويعد ذلك من العناصر الهامة في حوكمة تقنية المعلومات.

أفضل ممارسات إدارة الخدمات طبقاً لإطار آيتل ومنتدى إدارة خدمات تقنية المعلومات (ITSMF):

سبق الحديث في الفصل السادس من هذا الكتاب عن مكتبة البنية التحتية لتقنية المعلومات آيتل (ITIL) وعن معايير أفضل الممارسات الخاصة بها، وذلك فيما يتعلق بدعم وتقديم خدمات تقنية المعلومات. فهي تقوم بتوفير الإرشادات والدعم الفعال لكل من إدارة تقنية المعلومات في المؤسسة والعديد من المجالات المتعلقة بحوكمة تقنية المعلومات، فعمليات مكتبة البنية التحتية لتقنية المعلومات آيتل تغطي مجالات أكثر توافقاً مع عملية التشغيل التي تتسم بالسلاسة للبنية التحتية الشاملة لتقنية المعلومات. وعلى الرغم من إلقاء الضوء عليها مع العمليات الأخرى لأفضل الممارسات في الفصل السادس من هذا الكتاب، فإن فهم وتطبيق أفضل ممارسات إدارة مستوى الخدمات في آيتل يعد أمراً في غاية الأهمية خصوصاً هذه الأيام.

إن إدارة مستوى الخدمة Service level management هو الاسم المُعطى لعملية التخطيط، والتنسيق، والصياغة، والاتفاق، والرقابة، وإعداد التقارير فيما يخص الاتفاق الرسمي بين كل من إدارة تقنية المعلومات في المؤسسة ومقدمي ومتلقي خدمات تقنية المعلومات. وتأخذ هذه العمليات الصفة الرسمية من خلال إبرام اتفاقيات مستوى الخدمات SLAs بين تقنية المعلومات وعملاء أو المستخدمين للتطبيقات والعمليات والخدمات الأخرى الخاصة بتقنية المعلومات. أي أن هذه الاتفاقيات تمثل الاتفاق الرسمي بين مقدمي خدمات تقنية المعلومات وعملاء تقنية المعلومات. عندما تم نشر الإصدار الأول للمواد الخاصة بأفضل ممارسات مستوى الخدمة في آيتل عام ١٩٨٩، كانت اتفاقيات مستوى الخدمة SLA من المفاهيم المثيرة للاهتمام، إلا أنها لم تكن شائعة في ذلك الوقت. أما في الوقت الراهن فقد قامت العديد من المؤسسات بطرحها بالرغم من تفاوت درجات نجاحها، ويتعين على كبار المديرين أن يكونوا على دراية كافية بها ومدركين لأهميتها عند فهم الضوابط الداخلية للبنية التحتية لتقنية المعلومات.

وفي مثال على اتفاقيات مستوى الخدمة، عندما تقوم إدارة تقنية المعلومات في المؤسسة بالتعاقد مع مقدم خدمات خارجي على تقديم بعض الخدمات، مثل خدمة النسخ الاحتياطي الخاص بالتعافي من الكوارث، فإنه لا بد من تأمين وحماية هذه الاتفاقية من خلال عقد رسمي يتم من خلاله الحصول على موافقة مقدم خدمة التعافي من الكوارث على تقديم مستويات معينة من هذه الخدمة وفقاً لجدول زمني محدد يعتمد على وقت الاستجابة. وفي هذه الحالة يُطلق على العقد المنظم لهذا الاتفاق اسم اتفاقية مستوى خدمة SLA بين وحدة تقنية المعلومات ومقدم الخدمات المستمرة. وفي هذه الحالة تكون اتفاقيات مستوى الخدمة SLAs المبرمة بين إدارة تقنية المعلومات وعملائها أكثر أهمية من منظور الرقابة الداخلية. لقد قمنا باستخدام مصطلح "العميل" للدلالة على المصطلح القديم الذي لا يزال شائعاً حتى الآن ألا وهو "مستخدمو تقنية المعلومات". كما أن هناك مجموعات كثيرة في المؤسسة تستخدم مصطلح "خدمات تقنية المعلومات" IT's Services، وباعتبارهم عملاء لإدارة تقنية المعلومات، فإنهم يتوقعون مستويات معينة من الخدمة والاستجابة. ويتم تحديد وتعريف هذه الاتفاقيات من خلال ما يُعرف باتفاقية مستوى الخدمة SLA، وهي

عبارة عن اتفاق موثق بين إدارة تقنية المعلومات وعملائها يحدد الأهداف الرئيسية للخدمات والمسؤوليات المنوطة بكلا الطرفين. لذا لابد من التركيز على الاتفاقية، كما لا يجب أن تستخدم اتفاقيات مستوى الخدمة وسيلة لتهديد طرف أو آخر لإجباره على الاستجابة لمطالبه. نحن أيضاً لا نتحدث هنا عن وجود ضرورة رسمية أو شكل قانوني للوثيقة، ولكن نتحدث عن تفاهم موثق بين جميع الأطراف. لذلك لابد من عمل شراكة حقيقية بين مقدم خدمات تقنية المعلومات والعملاء للتوصل إلى اتفاقية ذات منفعة متبادلة. خلاف ذلك، ستفقد اتفاقية مستوى الخدمة أهميتها بشكل سريع وتكون هدفاً لتلقي اللوم وقد تمنع ثقافة إلقاء التهم في هذه الحالة حدوث أي تحسينات حقيقية على جودة الخدمات.

بناءً على اتفاقية مستوى الخدمة، تتعهد إدارة تقنية المعلومات بتقديم خدمات محددة طبقاً لكل مجموعة من الجداول الزمنية المتفق عليها، وعليها أن تتفهم أن هناك عقوبات جزائية إذا لم يتم تحقيق معايير الخدمة. إن الهدف من كل هذا هو المحافظة على جودة الخدمات وتحسينها من خلال دورة ثابتة من الاتفاق، والمتابعة، والإبلاغ، وتحسين المستويات الحالية لخدمات تقنية المعلومات. لذا يجب أن تركز اتفاقيات مستوى الخدمة بشكل إستراتيجي على الأعمال والحفاظ على المواءمة بين الأعمال وتقنية المعلومات.

يلخص الشكل التوضيحي (١٧-١) محتويات الاتفاقية النموذجية لمستوى الخدمة. وننوه هنا إلى أنه لا يجب أن تكون هذه الاتفاقية عبارة عن نوع من الوثائق التي تشبه وثيقة رهن منزل يتم التوقيع عليها على أنها جزء من عملية إتمام شراء المنزل، بل يقوم عملاء تقنية المعلومات باستخدامها في توثيق متطلبات خدمة تقنية المعلومات التي يسعون إليها مثل "ألا يزيد متوسط وقت الاستجابة عن ... " أو "المعالجة الخاصة بإقفال النظم المالية تتم بحلول ... " أو غيرها من العوامل. ولضبط التوقعات الخاصة بتلك الخدمات وعرض ما يمكن أن يكون متاحاً منها، فإن إدارة تقنية المعلومات تقوم عادة بتقديم بيان خاص بعروض خدمات تقنية المعلومات. لذا يجب إتمام التفاوض بشأن المتطلبات الخاصة بعملاء خدمات تقنية المعلومات ووضعها في اتفاقيات رسمية لمستوى الخدمة. كما يجب

مراقبة الأداء في مقابل هذه الاتفاقيات الخاصة بمستوى الخدمة بشكل مستمر وإرسال تقارير تتعلق بأدائها بشكل منتظم. حيث إن الإخفاق في تحقيق المعايير الخاصة باتفاقية مستوى الخدمة قد يؤدي إلى المزيد من المفاوضات والتعديلات المتعلقة بهذه الاتفاقية. وتوفر هذه العملية الخاصة باتفاقية مستوى الخدمة فوائد ومزايا لكل من الأعمال ووحدة تقنية المعلومات تشمل ما يلي:

- نظراً لأن وحدة تقنية المعلومات يجب أن تعمل على تحقيق المعايير التي تم التفاوض بشأنها، فإن خدمات تقنية المعلومات تميل إلى أن تكون ذات جودة أعلى، الأمر الذي يؤدي إلى أعطال أقل. ومن الواجب أيضاً أن تتحسن إنتاجية مستخدمي تقنية المعلومات.
- سيتم استخدام الموارد البشرية في تقنية المعلومات بشكل أكثر فاعلية عندما تقوم وحدة تقنية المعلومات بتقديم الخدمات التي تلبى التوقعات الخاصة بالعملاء بشكل أفضل.
- باستخدام اتفاقيات مستوى الخدمة، يمكن قياس الخدمات المقدمة وسيتحسن عموماً التصور الخاص بعمليات تشغيل تقنية المعلومات.
- إن وجود العقود الملزمة سيجعل الخدمات المقدمة من الأطراف الأخرى (طرف ثالث) أكثر قابلية للإدارة ويقلل أي احتمالية للتأثير السلبي على خدمات تقنية المعلومات التي يتم تقديمها.
- إن مراقبة جميع خدمات تقنية المعلومات الخاضعة لاتفاقيات مستوى الخدمة تساعد على تحديد نقاط الضعف التي يمكن تحسينها.

شكل توضيحي (١٧-١)

عينة لمحتويات اتفاقية مستوى خدمات تقنية المعلومات

<p>نظراً لعدم وجود نموذج أو صيغة موحدة لاتفاقية مستوى خدمات تقنية المعلومات، فلا بد من أخذ العناصر التالية في الاعتبار على أنها محتوى لمعظم اتفاقيات مستوى الخدمات:</p>
<p>صفحات مقدمة الاتفاقية:</p> <ul style="list-style-type: none"> • الأطراف المشاركة في الاتفاقية. • عنوان الاتفاقية ووصف بسيط عنها. • تواريخ: البداية والنهاية، والمراجعة. • نطاق الاتفاقية، الأمور المشمولة وغير المشمولة. • مسؤوليات كل من مقدم الخدمة والعميل. • وصف للخدمات المشمولة.
<p>ساعات الخدمة Service hours:</p> <ul style="list-style-type: none"> • الوقت الطبيعي اللازم لكل خدمة. (مثال ٢٤x٧ أو من الاثنين إلى الجمعة من الساعة ٨:٠٠ - ١٨:٠٠). • الترتيبات الخاصة بطلبات مد الخدمة متضمناً ذلك فترات الإشعار المطلوبة. (مثال: يجب أن يتم تقديم الطلب إلى مكتب الخدمة قبل حلول الثانية عشرة ظهراً لتمديد الخدمة في التوقيت المسائي، وقبل الثانية عشرة ظهراً يوم الخميس لتمديد الخدمة خلال عطلة نهاية الأسبوع). • فترات سماح لساعات خاصة (مثل: الإجازات العامة). • التقويم الزمني للخدمة.
<p>الإتاحة Availability:</p> <ul style="list-style-type: none"> • مستويات الإتاحة المستهدفة ضمن الساعات المتفق عليها. ويتم التعبير عنها عادة بالنسب المئوية. لذا يجب تحديد فترة وطريقة القياس والتي يمكن أن تعبر عن كامل الخدمة أو الخدمات الداعمة أو المكونات الحساسة أو الثلاثة معاً. ونظراً لصعوبة ربطها بالنسب المئوية المبسطة، فإنه يمكن قياس الإتاحة من حيث عدم قدرة العميل على تنفيذ أنشطة الأعمال الخاصة بالخدمة.

<p>موثوقية الخدمة Reliability:</p> <ul style="list-style-type: none"> • يتم التعبير عنها عادةً بعدد انقطاعات الخدمة أو بمتوسط الوقت بين الأعطال • Mean Time Between Failures (MTBF) أو بمتوسط الوقت بين حوادث النظم • Mean Time Between System Incidents (MTBSI).
<p>الدعم Support:</p> <ul style="list-style-type: none"> • ساعات الدعم (وهي تختلف عن ساعات الخدمة) متضمنةً ذلك الترتيبات اللازمة لتقديم طلبات تمديد الدعم. • فترات الإشعار المطلوبة (مثلاً: يجب تقديم الطلب الخاص بتمديد الخدمة خلال الفترة المسائية إلى مكتب الخدمة قبل الثانية عشرة ظهراً أو قبل الثانية عشرة ظهراً يوم الخميس لتمديد الخدمة خلال فترة عطلة نهاية الأسبوع). • فترات سماح لساعات خاصة (مثل: العطل والإجازات العامة). • الوقت المستهدف للاستجابة للحوادث سواء كان مادياً أم باستخدام وسائل أخرى (مثال: الاتصال الهاتفي أو البريد الإلكتروني). • الوقت المستهدف لحل الحوادث، وذلك في حدود أولوية كل حدث — حيث يختلف الهدف اعتماداً على أولوية الحوادث.
<p>الطاقة الإنتاجية Throughput:</p> <ul style="list-style-type: none"> • هي مؤشر على حجم الحركة والأنشطة الإنتاجية المحتملة. (مثال: عدد المعاملات التي يتم تنفيذها أو عدد المستخدمين الذين يعملون في الوقت نفسه أو حجم البيانات التي يتم نقلها عبر الشبكة).
<p>أوقات الاستجابة للمعاملات Transaction response times:</p> <ul style="list-style-type: none"> • الأوقات المستهدفة لمعدل أو أعلى وقت استجابة لمحنة عمل. (أحياناً يتم التعبير عنها باستخدام النسب المئوية كأن نقول ٩٥٪ في غضون ثانيتين).
<p>الأوقات المطلوبة لتبادل الدفعات Batch turnaround times:</p> <ul style="list-style-type: none"> • أوقات تقديم المدخلات وزمان ومكان تسليم المخرجات.

<p>التغيرات Changes:</p> <ul style="list-style-type: none"> • أهداف تخص الموافقة على طلبات التغيير (RFCs) Request For Changes ومعالجتها وتنفيذها، والتي تعتمد عادة على الفئة أو إلحاحية/ أولوية التغيير. • استمرارية وأمن خدمات تقنية المعلومات IT service continuity and security • الإشارة باختصار لخطط استمرارية خدمات تقنية المعلومات وكيف يتم استدعاؤها وتغطية أي قضية من القضايا وخصوصاً أي مسئولية من مسئوليات العميل. (مثال: النسخ الاحتياطي لأجهزة الحاسبات الشخصية المستقلة PCs وتغيير كلمات المرور). • تفاصيل تتعلق بأي أهداف تخص الخدمات التي يتم الاستغناء عنها أو تعديلها في حال وقوع كوارث (إن لم يكن هناك أي اتفاقية منفصلة لمستوى الخدمة فيما يتعلق بموقف كهذا). 	<p>المطالبات المالية Charging:</p> <ul style="list-style-type: none"> • تفاصيل عن الصيغة أو المعادلة formula الخاصة بالمطالبات المالية والفترات الزمنية لها (في حال كانت هناك مطالبات مالية). إذا كانت اتفاقية مستوى الخدمة تشمل العلاقة مع المصادر الخارجية التي يتم الاستعانة بها، فإنه يجب تفصيل المطالبات المالية في الملحق كونها يتم تغطيتها غالباً بأحكام المعلومات السرية.
<p>إعداد تقارير عن الخدمات ومراجعتها Service reporting and reviewing:</p> <ul style="list-style-type: none"> • محتوى، وتكرار، وتوزيع تقارير الخدمات وتكرار اجتماعات مراجعة الخدمة. 	<p>الحوافز/ الجزاءات المرتبطة بالأداء Performance incentives/penalties:</p> <ul style="list-style-type: none"> • تفاصيل عن أي اتفاقية تتعلق بالحوافز أو الجزاءات المالية اعتماداً على الأداء مقابل مستويات الخدمة المحددة. وعلى الأرجح أن يتم تضمين هذه المعلومات (الحوافز/ الجزاءات) في حال كانت الخدمات تقدم عن طريق منظمة خارجية (طرف ثالث). ومن الجدير بالذكر هنا هو أن الشروط الجزائية يمكن أن تتسبب بوجود صعوبات خاصة بها.

إن عملية إبرام اتفاقية مستوى الخدمة هي إحدى العناصر الهامة لعمليات تشغيل تقنية المعلومات. فإذا لم تكن المؤسسة تستخدم اتفاقيات رسمية لمستوى الخدمة، فإنه يتعين على الإدارة العليا التفكير في تنفيذ العمليات الرسمية لاتفاقيات مستوى الخدمة الموصى بها. حيث تستطيع اتفاقيات مستوى الخدمة أن تخلق بيئة جديدة كلياً داخل تقنية المعلومات. ولتتمكن جميع الأطراف من فهم مسؤولياتهم والتزاماتهم تجاه الخدمة

على نحو أفضل. هذا بالإضافة إلى اعتماد اتفاقية مستوى الخدمة أساساً لتسوية العديد من المسائل.

يجب على المهنيين الذين يسعون إلى توسيع مدى إدراكهم لإدارة خدمات تقنية المعلومات أن يستخدموا المصادر الخاصة بمنتدى إدارة خدمات تقنية المعلومات itSMF الذي تم الحديث عنه سابقاً. تعتبر هذه المنظمة غير الربحية لاعباً بارزاً في عمليات التطوير والتعزيز المستمر لمعايير أفضل الممارسات الخاصة بإدارة خدمات تقنية المعلومات. ويستطيع المسئول التنفيذي المهتم بتعلم المزيد أن يزور الموقع www.itsmfi.org للحصول على المزيد من المعلومات. وسوف تقود عملية البحث إلى مواقع وطنية مستقلة لكل دولة. فهي منظمة تقبل عضويات ولكن يستطيع المرء التسجيل للدخول بصفة ضيف والوصول إلى العديد من الوثائق والأوراق والمعلومات المتعلقة بالمؤتمرات والندوات القادمة. يهتم منتدى إدارة خدمات تقنية المعلومات itSMF بالترويج لأفضل ممارسات إدارة خدمات تقنية المعلومات الخاصة بمكتبة البنية التحتية لتقنية المعلومات آيتل كما أن له اهتماماً قوياً بمعايير أيزو ٢٠٠٠٠ (ISO 20000).

معايير المجموعة المفتوحة للامتثال والأخلاقيات OCEG:

إن المجموعة المفتوحة للامتثال والأخلاقيات OCEG عبارة عن منظمة صناعية غير ربحية تعمل على تطوير المعايير وتساعد المؤسسات في تحسين عمليات الحوكمة وإدارة المخاطر والامتثال الخاصة بها. ومن خلال الدعم الكبير المقدم لها من قبل صناعة التقنية، قامت هذه المنظمة بنشر العديد من "المعايير" مثل نموذج قدرة الحوكمة وإدارة المخاطر والامتثال GRC. قمنا بوضع كلمة معايير بين علامتي اقتباس نظراً لأن المجموعة المفتوحة للامتثال والأخلاقيات لا تمتلك صلاحية وضع المعايير كما هو موجود في معايير الجمعية الأمريكية للمحاسبين القانونيين AICPA أو حتى في بعض المواد الإرشادية الخاصة بالمنظمة الدولية للمعايير ISO التي تناولنا الحديث عنها في الفصل السابع من هذا الكتاب.

يعرض هذا القسم "الكتاب الأحمر" "Red Book" الخاص بالمجموعة المفتوحة للامتثال والأخلاقيات OCEG ونموذج قدرة الحوكمة وإدارة المخاطر والامتثال GRC الخاص بها. إن هذه المواد الإرشادية للمجموعة المفتوحة للامتثال والأخلاقيات تشبه إلى حد كبير المعلومات

الإرشادية الأخرى للحوكمة وإدارة المخاطر والامتثال وإطار حوكمة تقنية المعلومات التي يمكن العثور عليها في فصول أخرى من هذا الكتاب، ولكن مع اختلاف طفيف في التركيز أو النهج المتبع. إن استخدام المجموعة المفتوحة للامتثال والأخلاقيات لكلمة "المفتوحة" له معنى خاص بالنسبة لتقنية المعلومات، إذ يتبادل النظام المفتوح التغذية الراجعة مع البيئة الخارجية لكي يقوم بإجراء تحليل مستمر لتلك الردود وإعادة ضبط النظم الداخلية حسب الحاجة لتحقيق أهداف النظام، ومن ثم نقل هذه المعلومات الضرورية مرة أخرى إلى تلك البيئة الخارجية. وتختلف النظم المغلقة عن النظم المفتوحة بأن لها حدوداً محكمة تسمح بتبادل معلومات طفيفة مع الخارج. تبدو بعض المنظمات غالباً - مثل المنظمات البيروقراطية والاحتكارية ونظم تقنية المعلومات الكاسدة والتي قامت بغلق الحدود - غير صحية. فالمصطلح الشائع بالنسبة للعديد من نظم تقنية المعلومات الحديثة والمتطورة هذه الأيام، هو مصطلح "المفتوحة" وهي الكلمة المناسبة لنموذج قدرة الحوكمة وإدارة المخاطر والامتثال.

توجد الإرشادات الخاصة بالحوكمة وإدارة المخاطر والامتثال والصادرة عن المجموعة المفتوحة للامتثال والأخلاقيات في وثيقة أطلق عليها اسم "الكتاب الأحمر" الخاص بنموذج القدرة، وتوجد هذه الوثيقة في الموقع www.oceg.org. وللعلم فإن الوثيقة الرسمية في نسختها الثانية حتى وقت نشر هذا الكتاب، متاحة عبر شبكة الإنترنت، في حين أن النسخة المحسنة متاحة فقط للأعضاء المشتركين. تحتوي نسخة الإنترنت الأساسية على وصف كامل لنموذج الحوكمة وإدارة المخاطر والامتثال. لكن يمكن بتكلفة إضافية الحصول على النسخة المحسنة مع قوالب وغيرها من الوسائل المساعدة والمفيدة في تطبيق هذه الأداة. يستند نموذج القدرة هذا على مفهوم سُمي بالأداء القائم على مبادئ (Principled Performance)، وهو نهج متكامل للحوكمة وإدارة المخاطر والامتثال سنتحدث عنه في الأقسام اللاحقة.

تمثل صورة عناصر قدرة الحوكمة وإدارة المخاطر والامتثال الموضحة بالشكل (١٧-٢) قلب نموذج المجموعة المفتوحة للامتثال والأخلاقيات؛ إذ إن العديد من المفاهيم هنا تشبه إلى حد كبير مفاهيم الحوكمة وإدارة المخاطر والامتثال التي تحدثنا عنها في فصول أخرى من

هذا الكتاب، إلا أن نموذج المجموعة المفتوحة للامتثال والأخلاقيات له نظرة صناعية ومرتكزة على تقنية المعلومات بشكل أكبر. إن أهداف المجموعة المفتوحة للامتثال والأخلاقيات الخاصة بهذا النموذج يجب أن تساعد المؤسسات على عمل ما يلي:

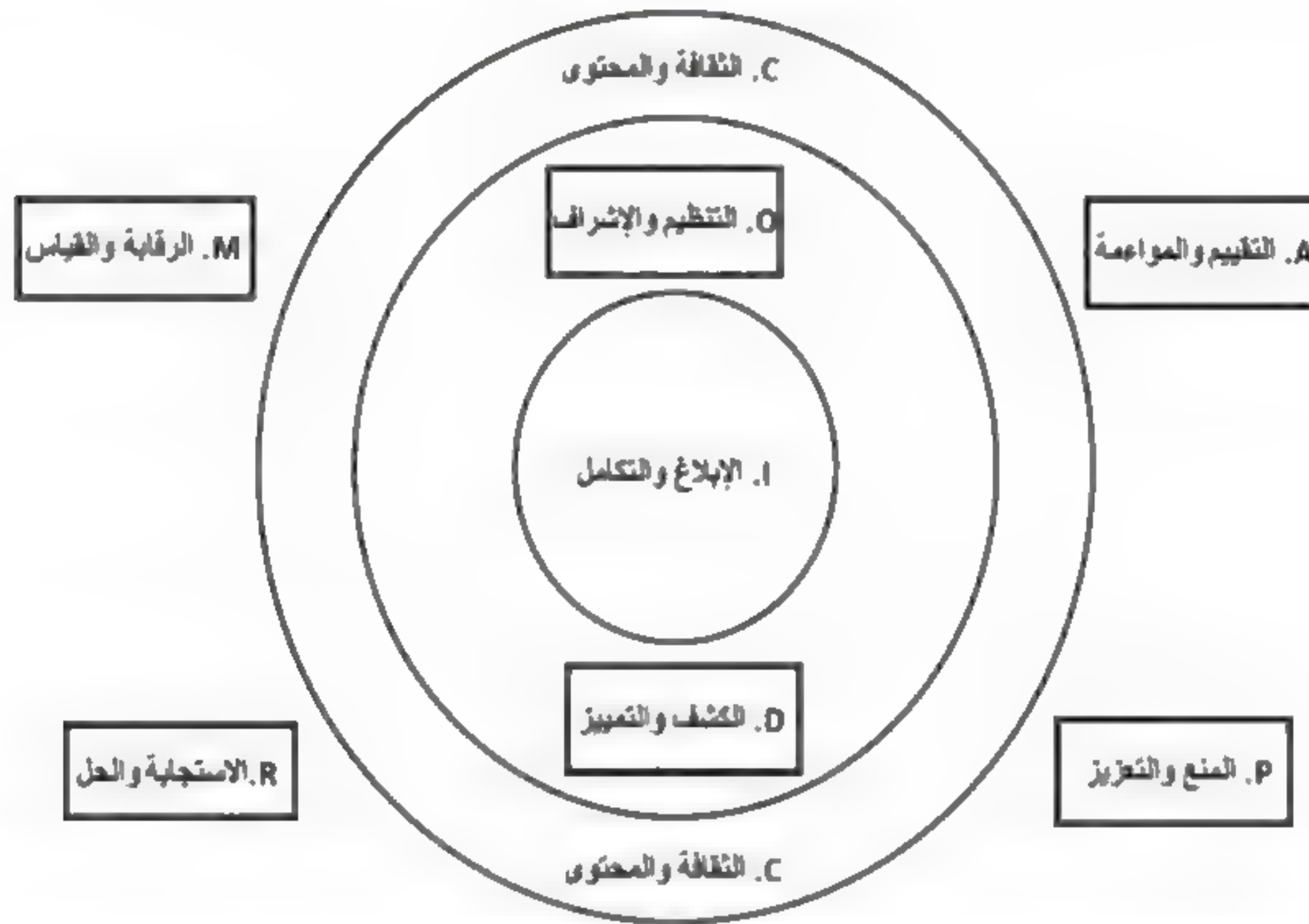
- تعزيز أهداف العمل.
- تعزيز ثقافة المنظمة.
- زيادة ثقة أصحاب المصلحة.
- تجهيز المؤسسة وحمايتها.
- منع وقوع الكوارث، والكشف عنها، وتقليصها.
- التحفيز والحث على السلوك المرغوب فيه.
- تحسين المسؤولية والكفاءة.
- تحسين القيمة الاقتصادية والاجتماعية.

مفهوم الأداء القائم على مبادئ الخاص بالمجموعة المفتوحة للامتثال والأخلاقيات OCEG:

لقد جعلت المجموعة المفتوحة للامتثال والأخلاقيات من مصطلح الأداء القائم على مبادئ علامة تجارية خاصة بها. حيث يصف هذا المصطلح الحاجة إلى صياغة الأهداف المالية وغير المالية للمؤسسة اللازمة لتحقيق جميع الأهداف التي تختارها المؤسسة للأخذ بها أثناء توظيف النهج الذي يتسم بالفاعلية والكفاءة والاستجابة لدعم أهداف كل من الحوكمة وإدارة المخاطر والامتثال. الفكرة هنا هي أن جميع المؤسسات يجب أن تعمل ضمن حدود داخلية وخارجية محددة، حيث تقوم القوى الخارجية بالمتطلبات القانونية والتنظيمية بإقامة الحدود الخارجية المفروضة. فالهدف هنا هو العمل على تكامل مبادئ وأهداف الحوكمة وإدارة المخاطر والامتثال لمساعدة المؤسسة على التحكم بالأداء على نحو أفضل.

شكل توضيحي (٢-١٧)

عناصر نموذج قدرة الحوكمة وإدارة المخاطر والامتثال GRC الخاصة بالمجموعة المفتوحة للامتثال والأخلاقيات OCEG



لكي تحقق المؤسسة مفهوم الأداء القائم على مبادئ Principled Performance الخاص بالمجموعة المفتوحة للامتثال والأخلاقيات، فإنه يجب عليها أن تحدد بوضوح رسالتها ورؤيتها وقيمها وأن تحدد أيضاً الأهداف التي تسعى لتحقيقها. كما يجب أن تحدد المؤسسة أيضاً كيف ستحقق أهدافها في الوقت الذي تتعامل فيه أيضاً مع المخاطر والإشكالات وحماية وخلق القيمة وتحديد فرص جديدة، والبقاء ضمن حدود معينة من السلوك الأخلاقي. كما يجب على المؤسسة أن تتحرى الشفافية في هذه الخيارات بالنسبة لأصحاب المصالح الداخليين والخارجيين، ويجب أن تحاول تحقيق جميع هذه الأمور باستخدام نهج متكامل لتحقيق أعلى مستوى ممكن من الأداء.

إن هذه المفاهيم للأداء المبدئي هي العناصر الرئيسية لنموذج قدرة الحوكمة وإدارة المخاطر والامتثال الخاصة بالمجموعة المفتوحة للامتثال والأخلاقيات كما هو موضح في الشكل التوضيحي (٢-١٧) والتي تم إعادة صياغتها من المواد الخاصة بالمجموعة المفتوحة للامتثال والأخلاقيات. الأقسام التالية تصف عناصر هذا النموذج بمزيد من التفصيل. يوجز هذا النموذج مجموعة كبيرة من المواد والمفاهيم الرفيعة المستوى التي تعتبر جزءاً من نموذج المجموعة المفتوحة للامتثال والأخلاقيات. نشجع القارئ المهتم بالوصول إلى كامل النموذج من خلال عنوان الويب المشار إليه سابقاً.

عناصر القدرة والبيئة والثقافة الخاصة بالحوكمة وإدارة المخاطر والامتثال GRC:

يعرض الشكل التوضيحي (٢-١٧) كلاً من القدرة والبيئة والثقافة على أنها عوامل أو عناصر في نموذج الحوكمة وإدارة المخاطر والامتثال الخاص بالمؤسسة. يهدف هذا الشكل إلى توضيح البيئة الداخلية والخارجية للأعمال والثقافة الحالية التي تعمل فيها المؤسسة. على سبيل المثال، يمكن لنظام الحوكمة وإدارة المخاطر والامتثال أن يعالج الأوضاع الراهنة وأن يحدد الفرص المتاحة للتكيف مع البيئة والثقافة لتحديد قيم المؤسسة من أجل تحقيق النتائج المرجوة بشكل أفضل. وباستخدام الحرف C نجد أن هناك أربعة عناصر خاصة بهذا المقطع من نموذج GRC المنشور وهي:

C1 سياق أو بيئة الأعمال الخارجية.

C2 سياق أو بيئة الأعمال الداخلية.

C3 الثقافة.

C4 القيم والأهداف.

يُعرّف نموذج قدرة الحوكمة وإدارة المخاطر والامتثال أيضاً مجموعة من العناصر الفرعية لكل عنصر من هذه العناصر. على سبيل المثال، يحتوي النموذج على العناصر الفرعية التالية للعنصر C3:

C3.1 تحليل الثقافة الأخلاقية.

C3.2 تحليل القيادة الأخلاقية.

C3.3 تحليل ثقافة المخاطر.

C3.4 تحليل إشراك مجلس الإدارة.

C3.5 تحليل ثقافة الحوكمة ونمط الإدارة.

C3.6 تحليل مشاركة القوى العاملة.

وكل عنصر من هذه العناصر الفرعية مدعوم بعناصر أكثر تفصيلاً لتوسيع الصورة. إضافة إلى ذلك، يحتوي النموذج على مجموعة من المبادئ وقائمة بمصادر الإخفاقات الشائعة لكل مبدأ من هذه المبادئ، هذا بالإضافة إلى احتوائه أيضاً على إرشادات ومراجع لمواد دعم إضافية.

عناصر القدرة والتنظيم والإشراف الخاصة بالحوكمة وإدارة المخاطر والامتثال GRC:

إن هدف الإرشادات الخاصة بالمجموعة المفتوحة للامتثال والأخلاقيات هو تنظيم ووصف نظام الحوكمة وإدارة المخاطر والامتثال الذي يتكامل مع عمليات الأعمال القائمة والذي يمكن أن يعدل فيها أيضاً عند الضرورة. أما تلك المجموعة من العناصر التي تمت الإشارة إليها بالحرف O في نموذج المجموعة المفتوحة للامتثال والأخلاقيات فهي تحتوي على العناصر الأساسية والفرعية التالية:

O1 النتائج والالتزام:

O1.1 تحديد نطاق نظام GRC.

O1.2 تحديد أنماط وأهداف نظام GRC.

O1.3 الحصول على الالتزام بنظام GRC.

O2 الأدوار والمسؤوليات:

O2.1 تحديد وتمكين قواعد الرقابة والمساءلة لنظام GRC.

O2.2 تحديد وتمكين أدوار ومسؤوليات الإدارة.

O2.3 تحديد وتمكين الأدوار والمسؤوليات القيادية.

O2.4 تحديد وتمكين القواعد التشغيلية لنظام GRC.

O2.5 تحديد وتمكين أدوار الضمان والمساءلة (مثل الرقابة الداخلية).

من خلال مخطط كهذا من النقاط الفرعية والنقاط المتفرعة منها، فإنه يوجد تفصيل كاف ليساعد المؤسسة على تأسيس وتنظيم وحدة أو إدارة للحوكمة وإدارة المخاطر والامتثال. فهناك مجموعة جيدة من المبادئ ومصادر الإخفاقات الخاصة بكل من هذه المبادئ للمساعدة في تنظيم عملية فعالة في الحوكمة وإدارة المخاطر والامتثال في المؤسسة. إن هدف هذا الفصل هو تسليط الضوء على أن نموذج القدرة للحوكمة وإدارة المخاطر والامتثال الخاص بالمجموعة المفتوحة للامتثال والأخلاقيات (OCEG GRC) يحتوي على بعض الأدوات الرائعة لمساعدة المؤسسة على تأسيس إدارة فعالة للحوكمة وإدارة المخاطر والامتثال وتحسين عمليات حوكمة تقنية المعلومات. فنحن هنا نسلط الضوء فقط على بعض الخصائص الرفيعة المستوى في هذا النموذج. فكل عنصر من هذه العناصر مدعوم بمزيد من التفاصيل.

لسنا هنا بصدد التوسع في الحديث عن نموذج المجموعة المفتوحة للامتثال والأخلاقيات OCEG والتعليق على كل عنصر من عناصره. بل نقوم فقط بتسليط الضوء على هذا النموذج للمجموعة المفتوحة للامتثال والأخلاقيات OCEG الذي يقدم بعض الإرشادات الرائعة لمراعاة بعض العناصر الهامة من أجل إيجاد أو وضع عمليات هامة لحوكمة تقنية المعلومات.

عناصر أخرى للمجموعة المفتوحة للامتثال والأخلاقيات OCEG:

بالتأمل في الشكل التوضيحي (١٧-٢)، سنرى أن كل قسم من أقسام هذا النموذج يحتوي على أهداف محددة خاصة به. على سبيل المثال، الهدف الإرشادي المعلن للقسم A من نموذج المجموعة المفتوحة للامتثال والأخلاقيات المسمى بالتقييم والمواءمة، هو تعزيز

الملف الخاص بالمخاطر في المنظمة من خلال محفظة من المخاطر والأساليب والأنشطة في هذا المجال. وتتضمن الإجراءات هنا تحديد المخاطر وتحليلها وتحسينها. على سبيل المثال، الهدف من تحديد المخاطر في النموذج المنشور هو "تحديد الأحداث والقوى والعوامل التي يمكن أن تؤثر في تحقيق أهداف الأعمال، متضمنة تلك التي تنشأ نتيجة عدم الامتثال للمتطلبات الموضوعة بمقتضى القانون أو المعايير أو السياسات الداخلية أو غيرها من الحدود".

بالتأمل في نموذج القدرة، وبالنظر إلى القسم P المسمى بالمنع والتعزيز. حيث يهدف هذا القسم إلى تشجيع وتحفيز السلوكيات المرغوب فيها ومنع الأحداث والأنشطة غير المرغوب فيها، وذلك باستخدام مزيج من الضوابط والحوافز. يحتوي هذا القسم على سبعة عناصر منها مدونات قواعد السلوك والضوابط الوقائية وعلاقات وحاجات أصحاب المصالح. سنسلط الضوء على عنصر آخر في نموذج قدرة الحوكمة وإدارة المخاطر والامتثال GRC ألا وهو القسم R المسمى بالاستجابة والحل. ويهدف هذا العنصر إلى الاستجابة للأحداث التي تنشأ نتيجة لعدم الامتثال والأحداث غير الأخلاقية أو إخفاقات نظام الحوكمة وإدارة المخاطر والامتثال. وذلك لتتمكن المؤسسة من حل كل قضية من القضايا العاجلة ومنع وحل القضايا المشابهة مستقبلاً بكفاءة وفاعلية أكبر. ويتكون هذا العنصر من خمسة مكونات:

R1 المراجعة والفحص الداخلي.

R2 الاستفسارات والتحقيقات الخاصة بالطرف الثالث.

R3 الضوابط التصحيحية.

R4 الاستجابة للأزمات والاستمرارية والتعافي.

R5 علاج نظام الحوكمة وإدارة المخاطر والامتثال GRC.

إن العديد من هذه الإجراءات يذهب إلى ما هو أبعد من خطوات حوكمة تقنية المعلومات التي تم وصفها في فصول أخرى من هذا الكتاب الخاصة بالتحقيق في المخالفات المتعلقة بالممارسات الأخلاقية وممارسات الامتثال الخاصة بالمؤسسة. على سبيل المثال،

بالنسبة للعنصر الفرعي R1 الذي يتناول موضوع المراجعات الداخلية، فإن التوجيه هو المراجعة والجاهزية للتحقيق في المزاعم والمؤشرات الدالة على سوء السلوك أو على إخفاقات في نظام الحوكمة وإدارة المخاطر والامتثال للوقوف على الحقائق والظروف المحيطة والأسباب الرئيسية وإيجاد الحلول المناسبة لها. القاعدة هنا هي أنه لا ينبغي لمجلس الإدارة والإدارة العليا أن يكونوا أبداً هم الطرف المصدوم، بل يجب أن يكونوا على دراية بأي قضية قد تؤثر بشكل كبير في المؤسسة حين وقوعها.

يدعو المعيار المؤسسة إلى وضع إجراءات وفريق عمل أساسي للتحقيق والبحث أكثر في الشكاوى أو في التقارير الخاصة بقضايا الامتثال والقضايا الأخلاقية، وكذلك القضايا التي تم الكشف عنها أثناء عمليات الرقابة المستمرة أو التقييم الدوري لنظام الحوكمة وإدارة المخاطر والامتثال. يستمر المعيار في الدعوة إلى وضع إجراءات قوية لوضع أمور معينة في بؤرة اهتمام الإدارة العليا أو مجلس الإدارة. كما يدعو أحد المعايير التوجيهية الأخرى المؤسسة إلى أن تقوم بمراجعة أي حوادث أو بيانات مُبلغ بها بشكل دوري، وذلك لتحديد التوجهات، أو مواطن المشاكل، أو الضوابط التي بحاجة إلى تنقيح. وعليه فإن الإجراءات المقترحة أقوى مما كنا نتوقع أن نجده في العديد من المؤسسات هذه الأيام.

وبمزيد من البحث في العناصر الست الرئيسية للحوكمة وإدارة المخاطر والامتثال، نجد أن عنصر المتابعة والقياس يقع في الركن العلوي الأيسر من الشكل. حيث يحتوي هذا العنصر على الإرشادات الخاصة بإسناد المسؤوليات الإدارية، وسلطة صنع القرار، والمساءلة من أجل تحقيق أهداف النظام. ويستخدم هذا العنصر الحرف M ويتكون من عناصر مراقبة وتقييم أداء برامج الحوكمة وإدارة المخاطر والامتثال والبدء بإجراء التحسينات على النظم إذا اقتضت الضرورة ذلك.

يقر هذا العنصر بأن نظام الحوكمة وإدارة المخاطر والامتثال لابد أن يكون مرناً بما فيه الكفاية للاستجابة السريعة للتغيرات الداخلية والخارجية التي تحدث في البيئة التي يعمل بها. وأن هذا النظام سيكون أكثر فاعلية في حال كانت المؤسسة تقوم بتحديد وتقييم التغيرات المتوقعة في الوقت المناسب لتخطيط التعديلات على النظم. كما يقر النموذج أيضاً بأن الفشل في الاستجابة لأي تغيرات ضرورية في السياق قد ينتج عنه فشل في معايير

حوكمة تقنية المعلومات وفي الضوابط الحساسة لنظام الحوكمة وإدارة المخاطر والامتثال. يدعو المعيار المؤسسة أن تقوم باستمرار بمراقبة التغيرات الداخلية والخارجية التي يمكن أن يكون لها تأثير مباشر أو غير مباشر أو تراكمي على المؤسسة. على سبيل المثال، قد تشمل التغيرات في المتطلبات الخارجية ما يلي:

- القوانين والقواعد واللوائح.
- التوجيهات والقرارات الإدارية.
- الأحكام القضائية الهامة.
- الإرشادات التنظيمية والادعائية.
- أنشطة متابعة الأوامر وفرضها.
- التزامات الجمعيات التجارية ومنظمات المعايير.

تشير هذه القائمة إلى تحديات خاصة بالمؤسسة - خاصة الكبيرة منها وذات الجنسيات المتعددة - والتي سوف تواجهها عند محاولتها القيام بمراقبة أحداث مثل القرارات الحكومية. في أغلب الأحيان يكون الأمر أكبر من أن يتم إسناد هذه المهمة الرقابية إلى مجموعة واحدة للقيام بهذه المهمة الرقابية، وذلك بسبب اتساع وتنوع المعلومات. لذلك لابد من وجود عمليات معمول بها تحفز الإدارة على اختلاف مستوياتها ومواقعها على إرسال تقارير بمجالات التحذير المحتملة إلى مجموعة الإدارة المركزية للحوكمة وإدارة المخاطر والامتثال للقيام بمزيد من التحقيقات وتخطيط الإجراءات.

القسم I أو الإبلاغ والتكامل هو آخر عنصر في نموذج الحوكمة وإدارة المخاطر والامتثال. وهو يقع في وسط النموذج الموضح في الشكل التوضيحي (١٧-٢) وهدفه العام يتمثل في الحصول على المعلومات الخاصة بنظام الحوكمة وإدارة المخاطر والامتثال وتوثيقها، وإدارتها لكي يتدفق بكفاءة أعلى وأسفل وعبر المؤسسة الممتدة من أصحاب المصلحة الخارجيين وإليهم. وهذا يدعو المؤسسة إلى تطوير وتطبيق مجموعة كبيرة من العمليات الخاصة بمعلومات نظام الحوكمة وإدارة المخاطر والامتثال كعمليات تصنيف المعلومات، والحصول عليها، وتخزينها، وإبلاغها. وعلى الرغم من أنه ليس من الضروري أن يكون لدى المؤسسة

نظام واحد في كل موقع، فإنه يجب أن تتناغم هذه العمليات من حيث تصنيفاتها وأشكالها وقدراتها على الاتصال.

إن بنية مجموعة نظم الدعم الخاصة بالحوكمة وإدارة المخاطر والامتثال يمكن أن تكون أحد العوامل الرئيسية لنجاح نظام معلومات الحوكمة وإدارة المخاطر والامتثال بالكامل، لكنها أيضاً يمكن أن تكون أحد التحديات الرئيسية لتحقيق النجاح. على غرار مبادئ COSO ERM التي تحدثنا عنها في الفصل الثامن من هذا الكتاب، فإنه يتعين على المؤسسة أن تحصل على كمية كبيرة من البيانات والمعلومات المختلفة والعمل على تصنيفها، كما يجب أن يكون لديها القدرة أيضاً على الحصول على تلك المواد لتحليلها والرد على الاستفسارات الواردة.

نموذج المجموعة المفتوحة للامتثال والأخلاقيات OCEG وحوكمة تقنية المعلومات:

إننا لم نصل بعد إلى النقطة التي عندها يمكن للمديرين ذوي الاختصاص استخدام محرك البحث جوجل في البحث عن "نظم مراقبة الامتثال لنموذج الحوكمة وإدارة المخاطر والامتثال GRC الصادر عن المجموعة المفتوحة للامتثال والأخلاقيات OCEG" للحصول على قائمة بالباعه المناسبين الذين يعرضون برمجيات نظم مراقبة الامتثال الخاصة بـ OCEG GRC نتيجة لعملية البحث. يوجد العديد من الأساليب للحلول إلا أن هناك القليل من الحلول الفردية الواضحة. أحد مجالات الحلول المحتملة يمكن أن نجدها في نظم السجلات الإلكترونية الطبية في المستشفيات (EMRS) Electronic Medical Record Systems. ويتم تسجيل كل نشاط من الأنشطة الخاصة بالمريض، بدءاً من نتيجة الفحوصات المعملية، إلى ملاحظات الطبيب، إلى الأدوية الموصوفة، والكثير غيرها على نظام EMRS بغرض استرجاعها فيما بعد من أجل الاستخدام الحالي لها أو لأغراض الأرشيف. يجب أن يحتوي نظام المعلومات الفعال لنموذج قدرة الحوكمة وإدارة المخاطر والامتثال على العديد من هذه العناصر.

لقد أوجزت الأقسام السابقة العديد من عناصر نموذج القدرة للحوكمة وإدارة المخاطر والامتثال الصادر عن المجموعة المفتوحة للامتثال والأخلاقيات OCEG GRC على مستوى

عالٍ للغاية. إلا أن هناك نماذج أخرى تدعو إلى اتباع نهج أكثر تفصيلاً وفي بعض الأحيان يكون أكثر اعتماداً على الضوابط الإدارية. في جميع الأحوال فإن وصفنا الرفيع المستوى هنا للموضوع لا يقدم دراسة كاملة بالشكل الذي يمكن أن نجده في ٢٤٠-صفحة من المنشور الخاص بالمجموعة المفتوحة للامتثال والأخلاقيات OCEG، وفي شكله الأساسي، مع المزيد من التفاصيل في وثيقة موسعة، مما يشجع القارئ المهتم للقيام بالمزيد من البحث والتحقيق في نموذج OCEG GRC.

إن زيارة موقع الويب الخاص بالمجموعة المفتوحة للامتثال والأخلاقيات سيسمح بالوصول غير المحدود إلى مجموعة متنوعة من المواد، بعضها للاطلاع والبعض الآخر مخصص للمشاركين. وهي المواد ذات الأهمية الخاصة مثل الكتاب الأحمر وهو عبارة عن وثيقة تقييم لدعم إرشادات نموذج القدرة الخاص بالمجموعة المفتوحة للامتثال والأخلاقيات. والغرض منه تزويد المختصين في مجال الحوكمة وإدارة المخاطر والامتثال بمجموعة عامة من الإجراءات المستخدمة في التقييم والتي تتفق مع نموذج قدرة الحوكمة وإدارة المخاطر والامتثال الموضح سابقاً، وكذلك إرشادات حول ما يمكن توقعه خلال عملية تقييم أي نظام للحوكمة وإدارة المخاطر والامتثال، مع مجموعة من الأهداف التي تساعد المؤسسة في تقييم فاعلية تصميم وتشغيل نظام الحوكمة وإدارة المخاطر والامتثال الخاص بها، وكذلك خفض تكلفة تلك التقييمات من خلال تقديم إجراءات محددة. كما يهدف هذا المنشور إلى رفع مستوى نضج وجودة العمليات الخاصة بالحوكمة وإدارة المخاطر والامتثال الخاص بالمؤسسة، وذلك من خلال تقديم المساعدة في وضع خطط تحسين محددة الأولوية وتوفير مصدر خارجي للحكم والاعتراف بهذه الممارسات.

مستوى ونطاق سلطة وضع المعايير للمجموعة المفتوحة للامتثال والأخلاقيات OCEG:

كما أكدنا سابقاً، فإن المجموعة المفتوحة للامتثال والأخلاقيات لا تمتلك حتى الآن سلطة وضع المعايير كما هو حال المنظمات الأخرى مثل PCAOB والأيزو ISO. هذا بالإضافة إلى أنه بالرغم من إصدارها للعديد من المواد الإرشادية القوية، فإن هذه المواد لا تزال تفتقر للقبول والاعتراف العالي المستوى من قبل الآخرين حتى الآن. ومع كل هذا، فإننا نشعر بأن أهمية المجموعة المفتوحة للامتثال والأخلاقيات والمواد الإرشادية الخاصة بها ستتمو في

السنوات القليلة القادمة نظراً لنمو الاهتمام بالعمليات الفعالة للحوكمة وإدارة المخاطر والامتثال وزيادة الحاجة إليها.

إن إحدى نقاط القوة الرئيسية للمجموعة المفتوحة للامتثال والأخلاقيات هي أنها منظمة تطوعية بالكامل تُدار من قبل أعضاء من المنظمات الراعية وقد تم تشكيل مجلس إدارة لها من هؤلاء الأعضاء. وتضم قائمة الرعاة كبرى شركات المحاسبة العامة مثل برايس ووترهاوس-كوبرس Pricewaterhouse-Coopers وجرانت ثرونتون Grant Thornton. هذا بالإضافة إلى العديد من الرعاة الرئيسيين من قادة صناعة تقنية المعلومات أمثال أوراكل Oracle وساب SAP وكذلك رعاة الصناعة الأمريكية في المقام الأول من شركات مثل عون Aon وهي إحدى الشركات الكبرى للتأمين ومتاجر التجزئة وول مارت Walmart. فإذا كان هناك أي قلق أو خوف، فمن الواضح بأنه سيكون متوقفاً على المنظمات الراعية وأعضاء اللجنة الخاصة بالمجموعة OCEG. فهذه المجموعة ليست أكثر من أن مقرها الولايات المتحدة وليست منظمة دولية بالمعنى الحقيقي. وفي عالمنا المفتوح هذه الأيام، نحن بحاجة إلى المزيد من التركيز على المواصفات العالمية.

قيمة تقنية المعلومات VAL IT: تحسين قيمة استثمارات تقنية المعلومات:

وُجِدَت جميع المؤسسات سواء كانت كبيرة أو صغيرة لتقدم قيمة للمستفيدين من خدماتها. وتواجه هذه المؤسسات تحدياً حرجاً وحساساً فيما يخص ضمان تحقيقهم للقيمة من استثمارات المعقدة والمتزايدة بدرجة كبيرة في موارد تقنية المعلومات. وقد قام معهد حوكمة تقنية المعلومات (ITGI) الذي تم تقديمه للمرة الأولى في الفصل الخامس من هذا الكتاب، بإصدار مجموعة من المواد المتعلقة بأفضل الممارسات التي أطلق عليها اسم «قيمة تقنية المعلومات»^(١) Val IT لمساعدة المؤسسة على علاج هذا التحدي وتحقيق قيمة من تلك الاستثمارات القائمة على تقنية المعلومات.

تحاول Val IT أن تعالج المشاكل المتعلقة بإدارة وحوكمة تقنية المعلومات التي تواجهها الإدارة على اختلاف مستوياتها. حيث إن تقنيات وممارسات تقنية المعلومات دائمة التغير والتكيف تبعاً لممارسات الأعمال الجديدة. فكثيراً ما تستثمر المؤسسات في النظم والإجراءات الجديدة والمنقحة مع قليل من التخطيط والبحث الإضافي، حيث سرعان ما تكتشف أن

هذه المبادرات الجديدة لا تعمل كما هو مأمول أو أنها تحتاج إلى استثمار حجمه أكبر بكثير مما هو متوقع. إننا نواجه هذا الموقف كثيراً على سبيل المثال، عندما يصاب المدير المالي التنفيذي بالإحباط جراء بعض القصور في النظم المالية الخاصة بالمؤسسة. فيقوم هو شخصياً بالبحث عن أفضل الحلول الممكنة في العروض التجارية المقدمة من الموردين، ثم يعمل على تشجيع إدارة تقنية المعلومات على تبني واعتماد هذا الحل. وفي ظل هذا الضغط من أحد أعضاء الإدارة العليا ولكن بقليل من البحث والتحقيق التفصيلي فيما يخص هذا الشأن، فإن المؤسسات في بعض الأحيان تبادر في استثمارات جديدة في تقنية المعلومات بتكاليف باهظة دون الحصول قيمة حقيقية من تلك الاستثمارات. يعد Val IT أحد أطر العمل التي تحتوي على أفضل الممارسات للحوكمة، وهذا يتفق إلى حد كبير مع إطار أهداف ضوابط المعلومات والتقنيات ذات الصلة (كوبت) والذي تم الحديث عنه في الفصل الخامس من هذا الكتاب. يتكون إطار العمل كوبت من مجموعة من المبادئ الإرشادية وعدد من العمليات الموصى بها والمرتبطة بتقنية المعلومات والتي تتفق مع هذه المبادئ والممارسات الرئيسية في الإدارة. في حين يشكل الإطار Val IT مجموعة كاملة من الأنشطة البحثية والمطبوعات والخدمات الإضافية التي تدعم الإطار الرئيسي لقيمة تقنية المعلومات Val IT كما هو موضح في الشكل التوضيحي (١٧-٣). وعلى الرغم من أن الإطار كوبت يحدد ممارسات جيدة "للوائل" التي تسهم في عملية خلق القيمة، فإن الإطار Val IT يحدد ممارسات جيدة لتحقيق "الغايات"، وذلك من خلال تزويد المؤسسات بالهيكل الذي تحتاج إليه لقياس ومراقبة وتحسين عملية تحقيق قيمة الأعمال من استثماراتاتها في مجال تقنية المعلومات.

إن العديد من المؤسسات هذه الأيام بغض النظر عن حجمها وإيراداتها وصناعاتها وموقعها وأنشطة أعمالها، تقوم باستثمارات واسعة النطاق في مجال نظم تقنية المعلومات وموارد تقنية المعلومات المرتبطة بها. ومع ذلك، وفي حالات كثيرة جداً، فإنه وببساطة لا يتم تحقيق تلك القيمة لتقنية المعلومات. على سبيل المثال، في عام ٢٠٠٧ أوضحت الدراسة التي أجرتها شركة جارتنر Gartner المتخصصة في أبحاث تقنية المعلومات أن ٢٠٪ من إجمالي النفقات في تقنية المعلومات قد تم إهدارها^(٢). وهذه النتيجة توضح أن إجمالي الهدر على الصعيد العالمي نحو ٦٠٠ مليار دولار أمريكي سنوياً. وفي دراسة مشابهة أجرتها شركة جولدمان ساكس Goldman Sachs عام ٢٠٠٩ على عدد من المديرين التنفيذيين

للمعلومات CIOs والمصنفين بأنهم أكبر ١٠٠٠ مدير تنفيذي للمعلومات، وجدت أن ما يقرب من ٤٠٪، في المتوسط من إجمالي النفقات في مجال تقنية المعلومات لا عائد منها على المؤسسة^(٣). النقطة الرئيسية هنا هي أن العديد من المؤسسات لا تقوم بقياس أو تقييم قيمة استثماراتها الجارية في مجال تقنية المعلومات. وهذا يعد خسارة كبيرة من منظور حوكمة تقنية المعلومات.

شكل توضيحي (٣-١٧)

إطار عمل قيمة تقنية المعلومات Val IT



تقدم المواد^(٤) الخاصة بالإطار Val IT الصادر عن معهد حوكمة تقنية المعلومات ITGI إرشادات خاصة بتقييم القيمة المكتسبة من استثمارات تقنية المعلومات. إن إيجاد قيم معتمدة على تقنية المعلومات، فضلاً عن أنها ليست بالأمر السهل، فإن معظم المؤسسات يظهر عليها واحد أو أكثر من الأعراض التالية التي تم تلخيصها واقتباسها من المواد المنشورة والخاصة بإرشادات الإطار Val IT.

• **مشاكل في تقديم القدرات التقنية:** إن إدارات تقنية المعلومات لدى العديد من المؤسسات ليست على مستوى كافٍ من النضج لتقوم بتقديم القدرات التقنية اللازمة لدعم العمليات التشغيلية للأعمال ولتمكين تغير الأعمال على نحو كاف وفعال. وهذا التحدي يسلط الضوء على ضرورة تحسين عمليات حوكمة وإدارة تقنية المعلومات إما قبل أو بالتزامن مع تقديم ممارسات إدارة القيمة.

• **محدودية أو عدم معرفة نفقات تقنية المعلومات:** في كثير من الأحيان نجد أن كبار المديرين في المؤسسة يفتقرون للرؤية الواضحة الكافية فيما يتعلق بالنفقات الخاصة بتقنية المعلومات، وكذلك الاستثمارات في مجال تمكين تقنية المعلومات في جميع الخدمات والأصول وغيرها من موارد تقنية المعلومات لديهم. ونجد في أغلب الأحيان أن صناع القرار يمكنهم فقط توقع حجم الإنفاق على الاستثمارات الخاصة بتقنية المعلومات وحجم الفائدة التي ستعود عليهم جراء هذا الإنفاق وما يمكن أن تكون عليه الجدوى الاقتصادية الكاملة جراء هذا الالتزام. ويتم تمويل النفقات غالباً من ميزانيات غير منسقة. مما يؤدي إلى ازدواجية وتضارب كبيرين في عملية طلب الموارد. هذا بالإضافة إلى أنه في كثير من الأحيان نجد أن الإدارة لا تركز على قضايا حساب التكاليف والتسعير الخاصة بتقنية المعلومات في مراجعاتها الخاصة بوضع ميزانيات تطبيقات تقنية المعلومات.

• **تنازل الأعمال عن عملية صنع القرار لصالح إدارة تقنية المعلومات:** عندما تكون الأدوار والمسؤوليات والمسؤوليات المتعلقة بإدارة تقنية المعلومات في المؤسسة غير واضحة، عندها ستقوم إدارات تقنية المعلومات بانتزاع مقعد القيادة، وتحديد الاستثمارات المطلوبة في مجال الأعمال المعتمدة على تقنية المعلومات التي يجب البدء بها، إذ إنها تقوم بوضع أولويات لتلك الاستثمارات من وجهة نظرها المحدودة، مما يؤدي بشكل غير صحيح إلى تجريد الأعمال من مسؤولياتها في تحديد الجدوى الاقتصادية والدفاع عنها والتي تستخدم لتبرير كل قرار من القرارات المتعلقة بالاستثمار في مجال تمكين تكنولوجيا المعلومات.

• **ضعف التواصل بين إدارات تقنية المعلومات والأعمال:** يعتبر التعاون الوثيق بين إدارات تشغيل تقنية المعلومات وإدارات الأعمال الأخرى بمثابة القضية الحاسمة في عملية خلق القيمة المكتسبة من تقنية المعلومات. فعند غياب مثل هذه الشراكة، سيتأثر التواصل،

وتتزايد أوجه القصور، ويظهر الفشل في أوجه التوافق في النشاط، وتأخذ ثقافة التنصل وإلقاء التهم واللوم في الانتشار داخل بيئة العمل. في بعض الحالات نجد أن إدارة تقنية المعلومات تتحول كثيراً إلى دور التابع بدلاً من دور المبتكر. كما يتم إشراكها في الاقتراحات الخاصة بالاستثمارات في وقت متأخر جداً عن عملية اتخاذ القرار لدرجة لا تستطيع معها أن تسهم في هذه الاستثمارات بقيمة كبيرة. وفي حالات أخرى يتم إلقاء اللوم على إدارة تقنية المعلومات لعدم تقديمها لقيمة من الاستثمارات الخاصة بتمكين تقنية المعلومات - وهي القيمة التي لا يمكن تحقيقها إلا من خلال الشراكة بين إدارة تقنية المعلومات وإدارات الأعمال الأخرى.

• **التشكيك في قيمة تقنية المعلومات:** مما يثير السخرية ، أنه على الرغم من استمرار المؤسسات في الاستثمار أكثر وأكثر في الموارد التقنية، فإن العديد من كبار المسؤولين التنفيذيين يتساءلون كثيراً حول ما إذا كانت القيمة المناسبة من هذه الاستثمارات قد تم تحقيقها بالفعل أم لا. حيث يكون التركيز الأكبر غالباً على إدارة التكاليف الخاصة بتقنية المعلومات بدلاً من فهم وإدارة ومحاولة الاستفادة من الدور الذي تلعبه إدارة تقنية المعلومات في عملية خلق قيمة ملموسة من الأعمال. فعندما تنطوي استثمارات تقنية المعلومات على تغيرات تنظيمية كبيرة وبشكل متزايد، فإن الفشل في تحويل التركيز من التكلفة إلى القيمة سيظل مستمراً ليكون هو العائق الأكبر أمام تحقيق القيمة المرجوة من هذه الاستثمارات المتعلقة بتقنية المعلومات.

• **إخفاقات كبيرة في الاستثمارات:** عندما تتعثر مشاريع تقنية المعلومات، فقد تكون تكاليف الأعمال المرتبطة بها هائلة ومرئية بشكل ملحوظ. حيث يمكن أن تؤدي عملية إلغاء المشاريع إلى آثار غير متوقعة ومكلفة جداً في الأعمال كما أن التجاوزات التي تحدث في الميزانية المخصصة يمكن أن تؤدي إلى حرمان المشاريع الأخرى من الموارد الحيوية الخاصة بها. وفي كثير من الأحيان يتم تجاهل هذه المشاكل حتى تصل إلى حد يكون فيه الوقت متأخراً لاتخاذ أي إجراء تصحيحي.

يمكن مشاهدة هذه الأعراض في العديد من إدارات تقنية المعلومات المؤسسية. ففي كثير من الأحيان نجد أن إدارة تقنية المعلومات تقود شركاءها في الأعمال من خلال الطلبات

الخاصة بوضع أولويات وطرح خدمات جديدة دون النظر إلى قيمتها الإجمالية التي ستعود على المؤسسة جراء تلك النفقات. لذا يجب أن تعمل مواد الإطار Val IT على تشجيع جميع المشاركين على أخذ نظرة أعمق على القيمة العائدة من استثمارات تقنية المعلومات وخدماتها. وربما الأهم من ذلك هو أن يعطي الإطار Val IT الفرصة لكبار المديرين للتركيز على المجالات المتعلقة بتحقيق قيمة أكبر من العمليات الخاصة بحوكمة عمليات تشغيل تقنية المعلومات.

إطلاق مبادرة لإدارة القيمة المكتسبة من تقنية المعلومات:

تم تصميم المواد الخاصة بإطار العمل Val IT الصادر عن معهد حوكمة تقنية المعلومات ITGI لتوفير الإرشادات لإدارات تقنية المعلومات في المؤسسة والإدارة العليا التي تقوم بتمويل موارد تقنية المعلومات وجميع أصحاب المصالح المستفيدين من تلك الأنشطة الخاصة بتقنية المعلومات. من ناحية أخرى، ونظراً لأن هذه الإرشادات الخاصة بأفضل الممارسات تنشر من قبل أحد المصادر ذات الصلة بجمعية ضبط نظم المعلومات وتدقيقها ISACA (وليس على سبيل المثال في أحد مطبوعات عضو مجلس إدارة في مؤسسة)، فإن هذه الإرشادات لم تلقَ الاهتمام اللازم والكافي من قبل الإدارة العليا. ومع ذلك يعد الإطار Val IT أحد مجموعات المواد الرائعة اللازمة لدعم حوكمة تقنية المعلومات ودعم عمليات تحسين الضوابط الداخلية.

يجب على الإدارة العليا أن تناقش المسائل المتعلقة بالقيمة المكتسبة من تقنية المعلومات مع كل من إدارة تقنية المعلومات وإدارة عمليات التشغيل. والتفكير في إطلاق مبادرة لإدارة القيمة المكتسبة من تقنية المعلومات. إن أحد أفضل الطرق لمعرفة جاهزية المؤسسة للبدء في برنامج لإدارة القيمة المكتسبة هي مراجعة وتقييم المبادئ الخاصة بالإطار Val IT ومدى التزاماته للعمل على تنفيذها. وتتضمن هذه المبادئ ما يلي:

- يجب أن تُدار استثمارات تقنية المعلومات كمحافظ استثمارية. كما وضحنا في الفصل الرابع عشر من هذا الكتاب.
- يجب أن تتضمن استثمارات تقنية المعلومات النطاق الكامل للأنشطة اللازمة لتحقيق القيمة المكتسبة للأعمال من هذه الاستثمارات.

- يجب إدارة استثمارات تقنية المعلومات من خلال دورات الحياة الاقتصادية الكاملة الخاصة بها.
 - ينبغي أن تعي جميع الممارسات الخاصة بتقديم القيمة في جميع أنحاء المؤسسة بأن هناك فئات مختلفة من الاستثمارات، ومن ثم فإنه يتم تقييم وإدارة تلك الاستثمارات بطرق مختلفة.
 - يجب على ممارسات تقديم القيمة أن تحدد وتراقب المقاييس الرئيسية، وأن تستجيب بشكل سريع لأي تغيرات أو انحرافات.
 - يجب على ممارسات تقديم القيمة إشراك جميع أصحاب المصالح في المسؤولية المناسبة وتقديم القدرات وتحقيق الفوائد الخاصة بالأعمال في ظل وجود المراقبة والتقييم وعمليات التحسين المستمرة.
- إن مديري تقنية المعلومات وكبار المديرين المعنيين بعمليات تقنية المعلومات الخاصة بالمؤسسة - أو يجب أن يكونوا - هم المعنيين بشكل مباشر بالإشراف على الممارسات الخاصة بإدارة القيمة أو تنفيذها. فاستناداً إلى المواد الخاصة بإطار Val IT، لا بد من عقد لقاء ما بين مديري تقنية المعلومات ومديري الأعمال في المؤسسة لتقييم مدى استعدادهم للانتقال نحو إدارة قيمة تقنية المعلومات. ويقدم الشكل التوضيحي (١٧-٤) مجموعة من الأسئلة والتأكيدات لمدى استعداد إدارة تقنية المعلومات لتقييم جاهزية المؤسسة للانتقال نحو إدارة تلك القيمة المتمثلة في تقنية المعلومات.
- يتعين على إدارة تقنية المعلومات التأمل في هذه الأسئلة والنقاط الموضحة بالشكل التوضيحي (١٧-٤) فيما إذا كانت المؤسسة وفريق إدارة عمليات التشغيل على علم بأهمية إدارة القيمة المكتسبة وأنهم قاموا باتخاذ الخطوات اللازمة نحو تطبيق هذا المفهوم. بكل تأكيد فإن جميع الأطراف - إدارة تقنية المعلومات وإدارة عمليات التشغيل - بحاجة إلى إقناعهم بأهمية إدارة القيمة المكتسبة من تقنية المعلومات.

شكل توضيحي (١٧-٤)

تقييم الجاهزية لإدارة القيمة المكتسبة من تقنية المعلومات

١. هل جميع استثمارات تقنية المعلومات سواء كانت تطبيقات أم شبكات أو الاتصالات الخاصة بالخواص، تدار كمحفظة استثمارية؟
٢. هل تتم إدارة جميع استثمارات تقنية المعلومات لتشمل النطاق الكامل للأنشطة المطلوبة لتحقيق أهداف الأعمال المرجوة من تلك الاستثمارات؟
٣. هل تدار استثمارات تقنية المعلومات من خلال دورات الحياة الاقتصادية الكاملة الخاصة بها، ابتداءً من تكاليف إطلاق الاستثمار أو شرائه مروراً بتكاليف التشغيل الاعتيادية وصولاً إلى نهاية الاستثمارات؟
٤. هل تدرك تقنية المعلومات والإدارة بأنه يجب أن يكون هناك فئات مختلفة من الاستثمارات المتعلقة بتقديم القيمة، حيث يجب أن تتم إدارتها وتقييمها بشكل مختلف؟
٥. هل لدى عملية تقديم القيمة مقاييس رئيسية تم تحديدها ومتابعة أي تغيرات أو انحرافات والرد عليها بشكل سريع؟
٦. هل يبدو على الممارسات الموضوعية لتقديم القيمة المكتسبة أنها تقوم بإشراك أصحاب المصالح وإسناد المساءلة المناسبة لتقديم القدرات وتحقيق المنافع والفوائد الخاصة بالأعمال؟
٧. هل هناك عمليات متابعة وتحسين مستمرة ومعمول بها على جميع الممارسات الخاصة بتقديم القيمة؟

تدعو الإرشادات المنشورة والخاصة بإدارة القيمة المؤسسية إلى أن تشارك بشكل أكبر في أفضل الممارسات الخاصة بإدارة القيمة. فهي تدعو المؤسسات وأصحاب المصالح ممن لديهم رؤية مبدئية فيما يخص إدارة القيمة إلى تطوير الفهم والوعي والالتزام بالمبادئ والممارسات الخاصة بإدارة القيمة. واستناداً إلى هذا التقييم المبدئي، يمكن البدء بتحليل أكثر تفصيلاً ونضجاً معتمداً على المجالات الخاصة بإطار قيمة تقنية المعلومات Val IT فيما يتعلق بحوكمة القيمة المكتسبة وإدارة المحافظ وإدارة الاستثمارات الخاصة بتقنية المعلومات.

الشروع في إدارة القيمة المكتسبة:

تعتبر المفاهيم الخاصة بإطار Val IT هامة بالنسبة للحوكمة الفعالة لتقنية المعلومات. ومن الطرق الفعالة للبدء في عملية إدارة القيمة المكتسبة تقييم الجاهزية الحالية من خلال استخدام أسئلة تقييم الجاهزية الموضحة في الشكل التوضيحي (١٧-٤). وبمجرد إتمام هذا التقييم، فإن النتائج ستقدم لنا الأساس اللازم لتحديد المطلوب إضافته من الحالة الحالية لإدارة القيمة المكتسبة إلى الحالة المستقبلية لها، ووضع أوليات لما يجب تطويره.

استناداً إلى المواد المنشورة الخاصة بإطار العمل Val IT والصادرة عن معهد حوكمة تقنية المعلومات ITGI، فإن الخطوات الخمس التالية تلخص كيف يمكن تطبيق إطار Val IT وإدارة القيمة المكتسبة في المؤسسة. وقد تكون الاختلافات بين المؤسسات كبيرة، لذلك فإن المواد الإرشادية الخاصة بإطار Val IT تصف فقط عدداً محدوداً من نقاط البدء.

خطوة (١): بناء الوعي والفهم لإدارة القيمة: نجد في العديد من المؤسسات أن صناع القرار وأصحاب المصالح الرئيسيين لا يقدرّون أهمية خلق القيمة المكتسبة أو الحاجة إليها كما يجب. فهذا المفهوم الخاص بالقيمة المكتسبة لا يظهر بشكل طبيعي من خلال خطط وأنشطة الأعمال الاعتيادية فحسب؛ بل يلزم أن يتشكل بفاعلية. ولعل المشكلة هنا تظهر في أنه على الرغم من أن مفاهيم إدارة القيمة المكتسبة موجودة منذ عقود، فإن فكرة إيجاد القيمة والحفاظ عليها من خلال تغيير الأعمال في المؤسسات الحديثة يكون التعامل معها عادة على أنها مبدأً ضمّني.

بالنسبة للعديد من المؤسسات لا يوجد هناك فهم موحد ومشترك لما يمكن أن يشكل قيمة للمؤسسة، وما مستوى العمل والجهد المطلوب لتحقيق تلك القيمة أو كيف يمكن قياس تلك القيمة. مما كان له بالغ الأثر في العديد من المؤسسات، وضياح أو فشل تنفيذ العديد من الفرص التي كان من شأنها إيجاد القيمة، مما أدى إلى تآكل مفهوم القيمة أو تدميره.

إن مديري العمليات التشغيلية والمديرين الماليين ومديري تقنية المعلومات في المؤسسة بحاجة إلى إيجاد قاعدة واسعة من الوعي بضرورة الحاجة إلى إدارة القيمة وتنشئة الوعي بها هو مطلوب لتطوير هذه القدرة، متضمناً ذلك التزامات داخلية قوية خاصة بالإدارة والسلطة التنفيذية لتحسين إيجاد القيمة والإبقاء عليها بمرور الوقت.

في ظل الفهم القوي لإدارة القيمة، يجب أن تتغير السلوكيات التنظيمية والفردية لإلقاء نظرة أوسع على مستوى المؤسسة بالكامل واتباع نهج أكثر انضباطاً واعتماداً على القيمة لصنع القرار. كل هذا من شأنه أن يؤدي إلى الإدراك والقبول المتزايد لضرورة أن تعمل إدارات تقنية المعلومات مع غيرها من إدارات الأعمال معاً في إطار من الشراكة المدعومة بأدوار، ومسئوليات ومسؤوليات واضحة تتعلق بإدارة القيمة، مما يقودنا إلى تحقيق قيمة أكبر من الاستثمارات الخاصة بتمكين تقنية المعلومات.

خطوة (٢): تطبيق حوكمة قوية لتقنية المعلومات: إن العمليات والأدوار والمسؤوليات والمسؤوليات المرتبطة بتحقيق القيمة المكتسبة من الاستثمارات الخاصة بتمكين تقنية المعلومات بحاجة إلى تحديد وقبول بشكل واضح. ففي كثير من الأحيان تكون الأدوار والمسؤوليات والمسؤوليات الخاصة بتقنية المعلومات غير واضحة إذا ما قورنت بغيرها من إدارات الأعمال. في بعض الأحيان يتم صنع القرارات المرتبطة بالأعمال من قبل إدارة تقنية المعلومات، في حين أن القرارات المرتبطة بتقنية المعلومات يتم صنعها من قبل الأعمال. في بيئة كهذه تكون ثقافة اللوم والتنصل وإلقاء التهم هي السائدة، وذلك في ظل الالتباس المستمر فيما يخص المساءلة والمسؤولية والرعاية.

تحتاج المؤسسة إلى وضع إطار عمل خاص بحوكمة تقنية المعلومات مع تحديد واضح للأدوار والمسؤوليات والمسؤوليات. وينبغي أن يكون هذا الإطار مدعوماً بقيادة قوية وملتزمة، وعمليات مناسبة، وهياكل ومعلومات تنظيمية، ونظام مكافآت ملائم. في ظل إطار لحوكمة المعلومات مثل هذا يجب أن تنمو التوجهات والسلوكيات التنظيمية، والفردية نحو رؤية أعمق وأكثر إستراتيجية للمؤسسة. لذا يتعين على المسؤولين التنفيذيين ومديري تقنية المعلومات وعمليات التشغيل أن يعتمدوا نهجاً أكثر انضباطاً واعتماداً على القيمة المكتسبة في اتخاذ قراراتهم ومسؤولياتهم. ففي ظل وجود حوكمة قوية لتقنية المعلومات، ينبغي أن تؤدي البيئة الأكثر كفاءة في صنع القرار إلى رفع مستوى الثقة بين إدارة تقنية المعلومات وباقي إدارات الأعمال الأخرى. وستكون النتيجة تحقيق قيمة أكبر من الاستثمارات الخاصة بتمكين تقنية المعلومات.

خطوة (٣): إجراء جرد لاستثمارات تقنية المعلومات: بالنسبة للعديد من المؤسسات، هناك رؤية ضعيفة، هذا إن وجدت، فيما يتعلق بعدد ونطاق وتكلفة الاستثمارات الخاصة بتمكين تقنية المعلومات الحالية والمخطط لها أو الموارد، سواء المخصصة للاستثمارات أم اللازمة لدعم تلك الاستثمارات. في كثير من الأحيان يكون إجمالي نفقات تقنية المعلومات في المؤسسة غير معلوم. وتأتي هذه النفقات غالباً من ميزانيات مختلفة وغير منسقة وبقدر كبير من الازدواجية. ففي العديد من المؤسسات يحدث عادة صراع كبير على طلب الموارد الخاصة بتقنية المعلومات.

ولحل هذه المشكلة لا بد للمؤسسة من إنشاء محافظ للاستثمارات والخدمات والأصول وغيرها من الموارد المتعلقة بتقنية المعلومات سواء كانت مقترحة أم فعلية. وهذا المفهوم أكبر حتى من أفضل الممارسات للإطار آيتل الخاصة بإدارة التهيئة والتي تمت مناقشتها في الفصل السادس من هذا الكتاب. ونتيجة لعملية إنشاء هذه المحافظ، لا بد أن يتغير السلوك والتوجهات التنظيمية والفردية لتشمل الرؤية الواسعة للمؤسسة، لذا لا بد من وجود العمليات والممارسات المعمول بها لدعم ذلك.

أهم الفوائد التي تعود من عملية جرد كهذه للاستثمارات الخاصة بتقنية المعلومات هي زيادة الفهم والإدراك لمعرفة ما تم إنفاقه بالضبط وعلى أية استثمارات تخص تقنية المعلومات، وفي أي مجال من مجالات الأعمال كانت تلك الاستثمارات، ومن هو المسؤول عنها. الفائدة الأخرى هي التحديد الأفضل للفرص لزيادة القيمة المكتسبة من خلال ضبط عملية تخصيص التمويل، والحد من التكلفة الإجمالية للمؤسسة عن طريق إزالة التكرارات، والاستخدام الأكثر فاعلية للموارد، وتقليل المخاطر من خلال الفهم الأفضل لتلك المحافظ الخاصة بتقنية المعلومات.

خطوة (٤): توضيح قيمة الاستثمارات الفردية لتقنية المعلومات: بالنسبة للعديد من المؤسسات إن لم يكن معظمها، لا توجد عملية تطبيقية تتم بشكل متناغم لتحديد قيمة الاستثمارات المحتملة أو الحالية لتقنية المعلومات. إنما يمكن تحديد هذه القيمة بأنها صافي إجمالي فوائد دورة الحياة من إجمالي تكاليف دورة الحياة المهيئة للمخاطر وعلى أساس القيمة الزمنية للأموال. ونتيجة لذلك، فإن بعض أصحاب المصالح يتساءلون باستمرار عما إذا كانت

استثمارات تقنية المعلومات قد أوجدت قيمة أم لا. تكون دراسة الجدوى الخاصة باستثمارات تمكين تقنية المعلومات غالباً غير موجودة أو سيئة الإعداد، ويتم التعامل معها عادة من قبل إدارة تقنية المعلومات على أنها مجرد مرجعية إدارية لازمة فقط لتأمين التمويل. يوجد القليل إن لم يكن لا شيء من معلومات ما قبل الاستثمار عن تكاليف تقنية المعلومات كما لا يوجد أي دقة في التحليل لتحديد تلك الفوائد أو القيمة. لا يوجد سوى القليل من المقاييس التي تمكن من متابعة ورصد القيمة التي بصدد الإنشاء أو التي تم إيجادها. في كثير من الأحيان نتصور أن التقنية أو إدارة تقنية المعلومات سوف تقدم قيمة سحرية.

يجب على المؤسسة أن تضع عملية خاصة بتطوير وتحديث دراسات الجدوى Business Cases الشاملة والمعدة بشكل ملائم فيما يتعلق بالاستثمارات الخاصة بتمكين تقنية المعلومات، متضمناً ذلك جميع النشاطات المطلوبة لخلق القيمة. كما يجب وضع دراسة الجدوى باستخدام نهج من أعلى - لأسفل. بدءاً من صياغة نتائج الأعمال المرجوة بشكل واضح واستكمالاً بوصف الإجراءات المطلوب إنجازها وعلى يد من ستم. كما أن دراسات الجدوى هذه يجب أن يتم تحديثها واستخدامها أداة تشغيلية خلال دورة الحياة الاقتصادية الكاملة الخاصة باستثمار تقنية المعلومات.

ونتيجة لهذه العملية، فإن التوجهات والسلوكيات التنظيمية والفردية لا بد أن تتغير لتكريس المزيد من الجهد المبذول للتخطيط لاستثمارات تقنية المعلومات وتطوير دراسات الجدوى وتحديثها بشكل مستمر. إن من شأن التقييم الأكثر موضوعية لدراسات الجدوى الخاصة باستثمارات تقنية المعلومات أنه يمكن من عمل مقارنات أفضل وأكثر موضوعية بين الأنواع المختلفة من الاستثمارات الخاصة بتقنية المعلومات. فهناك فرص أكبر لمقارنة الاستثمارات الفردية استناداً إلى قيمتها النسبية مقارنة بالاستثمارات الأخرى المتاحة وكذلك استناداً إلى مسار سجل Track record قوي لاختيار الأفضل. كما يجب أن يكون هناك أقل مستوى من عدم التأكد والمخاطر من أن القيمة المستهدفة لن تتحقق.

الخطوة (5): إجراء تقييمات وترتيب أولويات واختيارات لاستثمارات تقنية المعلومات: لا يوجد حالياً أي عملية تطبيقية مستمرة لإجراء تقييم موضوعي للقيمة النسبية لجميع استثمارات تقنية المعلومات المقترحة والحالية. خاصة فيما يتعلق بتحديد

الأولويات والاختيار من بين استثمارات تقنية المعلومات ذات القيمة المحتملة الأكبر. إن العديد من القرارات الاستثمارية الخاصة بتقنية المعلومات في المؤسسة هذه الأيام غير موضوعية وتكون سياسية غالباً. فمجرد اتخاذ القرار بالماضي قدماً في استثمار ما، فمن النادر جداً إعادة النظر فيه ما لم تحدث بعض الأزمات الحرجة. إذ يتم نادراً علاج أو إلغاء استثمارات تقنية المعلومات السيئة التنفيذ في الوقت المناسب والكافي للتقليل من الخسائر. فإذا تم إلغاؤها، فإنهم ينسبون الفشل إلى شخص ما ويجب تحميله المسؤولية ومحاسبته.

إن الحل الخاص بإطار العمل Val IT هو تطبيق نظم إدارة المحافظ لتصنيف استثمارات الأعمال المعتمدة على تقنية المعلومات. كما يجب على المؤسسة أن تُنشئ معايير وتقوم بتطبيقها بصرامة لدعم عمليات التقييم المتنوعة والمتجانسة للاستثمارات طوال دورة حياتها الاقتصادية بالكامل. ونتيجة لذلك، فإن التوجهات والسلوكيات التنظيمية والفردية يجب أن تتغير لتشمل النظرة الواسعة لدى المؤسسة وتبني مزيد من الشفافية.

إن الفائدة من هذا النهج المكون من الخطوات الخمس هي الفرص المتزايدة لخلق القيمة من خلال اختيار استثمارات تقنية المعلومات الأكثر احتمالاً لتقديم القيمة. ويجب أن تتبع هذه الفرصة إدارة فعالة لتلك الاستثمارات والإلغاء المبكر للاستثمارات التي يبدو أنها لن تستطيع أن تحقق القيمة المرجوة. وتقدم مواد الإطار Val IT المزيد من التفاصيل المرتبطة بتلك المنهجيات.

يقدم الإطار Val IT إرشادات مفيدة وعمليات وممارسات مجربة في حوكمة واختيار وإدارة الاستثمارات الخاصة بتمكين تقنية المعلومات. ويصف الإطار Val IT العمليات المترابطة التي من الضروري أن تكون في موضع التنفيذ إذا ما أرادت المؤسسات أن تضمن القيمة المكتسبة الأمثل من استثماراتهما. لم يرق هذا القسم إلا بتسليط الضوء واستخراج بعض المواد من المواد الإرشادية الخاصة بقيمة تقنية المعلومات. إن إطار Val IT هو أحد المفاهيم الخاصة بحوكمة تقنية المعلومات، وهو مفيد للغاية في تقييم القيم النسبية لتقنية المعلومات الموجودة في عمليات إطلاق التطبيقات الجديدة لتقنية المعلومات وبناء الضوابط العامة للإدارة. الأهم من ذلك هو ضرورة وصول تلك المفاهيم الخاصة بقيمة تقنية المعلومات إلى إدارة تقنية المعلومات والإدارة العليا ليتمكنوا من فهم استثماراتهم في موارد تقنية المعلومات على نحو أفضل.

ملاحظات:

- 1- Val IT Framework for Business Technology Management, www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-Pages/Val-IT1.aspx?utm_source=multiple&utm_medium=multiple&utm_content=friendly&utm_campaign=va.
- 2- IT Financial Management, Gartner Consulting, www.gartner.com/it/products/consulting/GTACaseStudy.pdf. f
- 3- Independent Insight: IT Spending Survey, “2009 Under the Knife—Expect -1% Global Decline,” Goldman Sachs, November 2, 2009, www.scribd.com/doc/7737986/Goldman-Sachs-IT-Spending-Survey.
- 4- John Thorp, “Val IT Framework 2.0—Adding Breadth and Depth to the Value Management Road Map,” ISACA Journal (June 2008): 1–3.

الجزء الخامس

متابعة وقياس حوكمة إدارة المؤسسة ومجلس الإدارة

03A

الفصل الثامن عشر

إدارة محتوى المؤسسة

يصف مصطلح إدارة محتوى المؤسسة ECM، وهو أحد مصطلحات إدارة تقنية المعلومات التي لم تكن شائعة حتى السنوات الأولى من القرن الحالي، الإستراتيجيات والأساليب والأدوات المستخدمة لحيازة وإدارة وحفظ وتقديم المحتوى والوثائق ذات الصلة بالعمليات التنظيمية. وقد أصبحت الآن إحدى المجموعات الخاصة بأنشطة تقنية المعلومات التي تشهد نمواً سريعاً، فإدارة محتوى المؤسسة عبارة عن سلسلة من العمليات التي تغطي إدارة المعلومات داخل نطاق المؤسسة بالكامل بغض النظر عما إذا كانت تلك المعلومات على هيئة وثائق ورقية أو ملفات إلكترونية أو بيانات مطبوعة من قاعدة البيانات أو رسائل البريد الإلكتروني أم بيانات مخزنة في البيئة السحابية لتقنية المعلومات أو على أي هيئة من الهيئات العديدة الأخرى المتطورة للمعلومات والبيانات. وتهدف عمليات إدارة محتوى المؤسسة في المقام الأول إلى إدارة دورة حياة المعلومات ابتداءً من إنشائها مروراً بأرشفتها وحتى التخلص منها في نهاية المطاف.

تهدف إدارة المحتوى المؤسسي إلى جعل إدارة معلومات الشركات والوثائق الداعمة لها أكثر سهولة، وذلك من خلال تبسيط تخزينها وأمنها وضبط إصداراتها وتوجيه معالجتها والقدرة على الاحتفاظ بها. إن الفوائد التي تعود على المؤسسة جراء استخدامها للعمليات الفعالة لإدارة المحتوى تتضمن كفاءات محسنة وضوابط أفضل وتكاليف أقل. على سبيل المثال، تستخدم معظم البنوك هذه الأيام عمليات إدارة المحتوى المؤسسي للاحتفاظ بالنسخ الورقية من الشيكات القديمة بدلاً من الطريقة القديمة لحفظ الشيكات الورقية في مستودعات ورقية ضخمة. فطبقاً للأنظمة القديمة والتقليدية، فإن طلب العميل الخاص بالحصول على نسخة من شيك قد يستغرق عدة أسابيع، حيث كان يجب على موظفي البنك الاتصال بالمستودع لمخاطبة شخص كان دوره تحديد موقع الصندوق والملف والشيك المطلوبين ومن ثم يقوم بسحب الشيك وعمل نسخة منه ومن ثم إرساله إلى البنك من خلال البريد، والذي يقوم في النهاية بإرساله إلى العميل بواسطة البريد. أما في حال وجود نظام لإدارة المحتوى المعمول به

في المؤسسة فإن موظف البنك يستطيع بكل بساطة أن يقوم بالبحث في النظام عن حساب العميل ورقم الشيك المطلوب. وبمجرد ظهور صورة الشيك على شاشة الحاسب، يستطيع الموظف إرساله فوراً إلى العميل عبر البريد الإلكتروني، وذلك أثناء انتظار العميل على الهاتف. تستطيع العمليات الفعالة لإدارة المحتوى المؤسسي أن تعمل على خفض التكاليف وتحسين العمليات، سواء كانت هذه العمليات تخص الشيكات في أحد البنوك أو أي مجموعة متنوعة من الوثائق الورقية الأخرى. إن العمليات الفعالة لإدارة المحتوى المؤسسي تعد من الأدوات الهامة التي تساعد في تعزيز حوكمة تقنية المعلومات في المؤسسة. يقدم هذا الفصل المفاهيم الخاصة بإدارة المحتوى المؤسسي ECM ويناقش المجالات التي يستطيع المدير التنفيذي من خلالها تحسين جميع عمليات حوكمة تقنية المعلومات من خلال تطبيق عمليات إدارة المحتوى المؤسسي

خصائص إدارة المحتوى المؤسسي ومكوناتها الرئيسية في المؤسسة اليوم:

تشتمل العوامل التي تشجع الأعمال والشركات على تبني واعتماد الحلول الخاصة بإدارة المحتوى المؤسسي على جميع الاحتياجات اللازمة لزيادة كفاءة المعاملات الخاصة بالأعمال، وتحسين ضبط المعلومات، وخفض التكلفة الإجمالية لإدارة المعلومات بالنسبة للمؤسسة. حيث تعمل تطبيقات إدارة المحتوى في المؤسسة على تسهيل الوصول إلى السجلات من خلال عمليات البحث باستخدام الكلمات الرئيسية والنص الكامل، الأمر الذي يسمح للموظفين بالحصول على المعلومات التي يحتاجون إليها مباشرة من مكاتبهم خلال ثوانٍ قليلة بدلاً من البحث في تطبيقات متعددة أو استخراجها من السجلات الورقية.

تستطيع نظم إدارة محتوى المؤسسة تعزيز ضبط ومراقبة السجلات لمساعدة المؤسسات على تحسين عمليات خدمة العملاء والامتثال للوائح الحكومية والصناعية مثل متطلبات قانون ساربنز أوكسلي SOX، التي تمت مناقشتها في الفصل الثاني من هذا الكتاب أو معيار أمن بيانات صناعة بطاقات الدفع (PCI DSS)، والذي جاء ذكره في الفصل الحادي عشر من هذا الكتاب. وتعد المهام الأمنية سواء كانت على مستوى المستخدم أو الإدارة، والخيارات الأمنية الخاصة بسجلات البيانات كذلك من المكونات الهامة في نظام إدارة المحتوى المؤسسي وذلك لحماية البيانات الحساسة.

كما يستطيع نظام إدارة المحتوى المؤسسي أن يقلل من الاحتياجات التخزينية والورقية والبريدية، ويزيد من كفاءة الموظفين، كما يؤدي أيضاً إلى قرارات مؤسسية أفضل وأكثر استنارة ووعياً، وكلها أمور من شأنها أن تقلل من التكاليف الإضافية لإدارة المعلومات. يعد نظام إدارة المحتوى المؤسسي ضرورياً وهاماً خاصة بالنسبة للمؤسسة التي لديها متطلبات لها علاقة بالاحتفاظ طويل الأجل بالمستندات والمتطلبات الخاصة بالاحتفاظ بأحجام كبيرة من المستندات. وفي ظل احتياجاتنا لوثائق مخصصة، يمكن لنظام إدارة المحتوى أن يساعد من خلال عمليات مدعومة بالتوقيع أو إدارة أصول رقمية لوسائط غنية أو إدارة تصاميم تقنية أو ضخمة الصياغة وغير ذلك.

من ناحية أخرى، فإن نظام إدارة المحتوى المؤسسي لا يعد من الأنظمة المغلقة أو من فئة المنتجات الفريدة أو المتميزة. وتُستخدم عبارة عمليات إدارة المحتوى المؤسسي مصطلحاً جامعاً يشير إلى مدى واسع من التقنيات الموضوعة في المؤسسة والموردين الذين يتعاملون معها. ويعمل نظام إدارة المحتوى المؤسسي بشكل مناسب عندما يكون "غير مرئي" بصورة فعالة بالنسبة للمستخدمين. وتقوم تقنيات نظام إدارة المحتوى المؤسسي بدعم تطبيقات مخصصة مثل الخدمات الفرعية، وتكون تلك التقنيات غالباً عبارة عن مجموعة من المكونات الخاصة بالبنية التحتية التي تناسب النماذج ذات الطبقات المتعددة وتتضمن جميع التقنيات المرتبطة بالوثائق والسجلات الموجودة في المؤسسة لمعالجة وتقديم وإدارة كل من البيانات المركبة والمعلومات غير المركبة معاً. وعلى هذا النحو، فإن عمليات نظام إدارة المحتوى المؤسسي تعد إحدى المكونات الرئيسية والضرورية في مجال تطبيق الأعمال الإلكترونية الشاملة.

عمليات إدارة المحتوى المؤسسي وحوكمة تقنية المعلومات:

تعد إدارة محتوى المؤسسة إحدى الإستراتيجيات المستمرة والمتطورة للوصول إلى رفع مستوى كيفية استخدام جميع معلومات المؤسسة إلى الدرجة القصوى. حيث تسمح أدوات وإستراتيجيات إدارة المحتوى المؤسسي للمؤسسة بإدارة كل من البيانات والمعلومات المركبة وغير المركبة الخاصة بأعمال المؤسسة بصرف النظر عن أماكن وجودها. وبالطبع فإن القيام فقط "بإدارة" هذا المحتوى من المعلومات لا يُعد أمراً كافياً. فالقدرة على

الوصول إلى الإصدار الصحيح لإحدى الوثائق أو السجلات يُعدُّ من الأمور الهامة، ولكن يجب إدارة هذا المحتوى لكي يتم استخدامه بالشكل الذي يحقق أهداف الأعمال. ومن الممكن أن تكون الأدوات والتقنيات الخاصة بإدارة المحتوى المؤسسي هنا ضرورية وهامة للقيام بإدارة كامل دورة حياة المحتوى الوثائقي منذ إنشائه وحتى التخلص منه.

إن إدارة المحتوى المؤسسي عبارة إستراتيجية مستمرة ومتطورة لزيادة الكيفية التي يجب من خلالها استخدام هذا المحتوى المعلوماتي للمؤسسة والذي قد يكون أساسياً لنجاح العمليات التشغيلية لأعمال المؤسسة. وعلى الرغم من وجود العديد من البرمجيات والعروض الأخرى التي يقدمها الموردون، فإنه يجب على الإدارة أن تفكر في تنفيذ واستخدام نظام إدارة المحتوى المؤسسي من حيث مفاهيم الامتثال والتعاون والاستمرارية والتكلفة.

على الرغم من حقيقة أن المؤسسات اليوم تواجه زيادات هائلة في أحجام ومستوى تعقيد أعمالها ونظمها، فإن العديد منها لا يزال يستخدم الطرق التقليدية القديمة نفسها القائمة على التعامل مع الوثائق واحدة تلو الأخرى. وقد تفتن المؤسسة إلى أن بعض الكفاءات وعمليات حوكمة تقنية المعلومات قد تتحسن من خلال اعتماد عمليات إدارة المحتوى المؤسسي للمؤسسة. وكنقطة انطلاق فإنه يتعين على الإدارة أن تقوم بمراجعة دورة حياة محتوى الوثائق لديها. إن هذه الفكرة مشابهة لحديثنا عن دورات حياة تطوير النظم (SDLCs) التي تناولها الفصل الخامس عشر من هذا الكتاب. لكن يجب أن يقوم هنا كل من فريق تقنية المعلومات والإدارة بوضع خريطة تفصيلية لمجريات تدفق أو سير العمليات الخاصة بالوثائق والمعلومات الحالية لمعرفة الأماكن التي يمكن أن يجدوا فيها تداخلات، وكذلك المجال الذي يمكن من خلاله التحسين في الإستراتيجيات الخاصة بتطبيقات الأعمال وتدفق المعلومات.

تُظهر المعلومات التي تم جمعها حجم التعقيدات الكامنة في العمليات التي تتعامل مع إدارة محتوى منظمة ما. لذا يجب أن يكون الهدف هو بناء معمارية لإدارة المحتوى في المؤسسة. كما هو موضح في الشكل التوضيحي (١٨-١)، والذي قد يشمل العديد إن لم يكن كل من العناصر التالية:

• **استحواذ نظام إدارة المحتوى المؤسسي (ECM) على جميع الوثائق:** يجب أن تركز عمليات إدارة المحتوى المؤسسي على حفظ وتتبع واستخدام المستندات كافة، سواء كانت وثائق ورقية أم رقمية أو وثائق لوسائط غنية كالفيديو أو الشعارات أو الصور. كما يجب أن تتعامل مستودعات الوثائق مع الوثائق المهيكلة وغير المهيكلة، مع الإقرار بأن تلك الأصول الرقمية يكون لها قيمة عالية من الملكية الفكرية. ومن الممكن أن يكون مستودع الوثائق عبارة عن نظام ضخم ومعقد ويكلف مئات الآلاف من الدولارات، أو يكون نظاماً بسيطاً كنظام الملفات والمجلدات المستخدم في شركة صغيرة. والمهم أن يكون لديهم معلومات يمكن العثور عليها بمجرد أن يتم وضعها في النظام.

• **خبرة المستخدمين وأدوات التشارك:** التعاون هو فن العمل بشكل جماعي. ويعد ضرورياً بالنسبة للتقنيات المرتبطة بإدارة المحتوى المؤسسي مثل الرسائل الفورية وألواح الكتابة (السبورات) والاجتماعات التي تتم عبر الإنترنت، ووسائل البريد الإلكتروني التي تسمح بإتمام العمل أينما وعندما يكون هناك حاجة إليه. ويسمح التعاون لأفراد بخبرات متكاملة أو متداخلة أن يقدموا نتائج أفضل وأسرع من ذي قبل، الأمر الذي يسمح لوحدة التشغيل وفرق الأعمال بالعمل سوياً في أي وقت، سواء كانوا في مكاتب متجاورة أم منفصلين بعضهم عن بعض في أي مكان في العالم.

• **دورات حياة سير العمل:** تعد الأدوات ضرورية لنقل المحتوى طيلة الدورات المحددة لعمليات العمل، كالعمليات اللازمة لمعالجة المطالبات. ولا بد من استخدام أدوات إدارة المحتوى المؤسسي في تطوير ونشر ومراقبة وتحسين عدة أنواع من التطبيقات الآلية. ويتضمن ذلك العمليات التي تشتمل على كل من النظم والناس. ترتبط دورات حياة سير الأعمال أيضاً مع العمليات اليدوية لإدارة الوثائق، كما يجب على دورات سير العمليات معالجة الموافقات وتحديد الأولويات التي يتم بناء عليها ترتيب الوثائق والمستندات التي يتم تقديمها. وفي الحالات الاستثنائية يقوم مخطط سير الأعمال بتصعيد قرارات مبنية على قواعد محددة سلفاً قد تم وضعها من قبل مالكي النظام.

• **إدارة السجلات الخاصة بنظام إدارة المحتوى المؤسسي:** في حين أن أي جزء من المحتوى يمكن تسميته سجلاً. إلا أنه يجب التعامل مع هذه العناصر وفقاً لجدول زمني للاحتفاظ

بها والذي يحدد المدة التي يتم الاحتفاظ خلالها بالسجل، ويكون ذلك بناء على اللوائح النظامية أو الممارسات التجارية الداخلية. كما أن هناك احتياجات لتخزين هذه السجلات المتعددة والمتنوعة بحيث يمكن استرجاعها عند الحاجة، وحذفها في نهاية المطاف في الأوقات المناسبة لاحقاً.

• **أدوات محتوى الويب، الوسائط الغنية:** يجب أن تقوم عمليات إدارة المحتوى المؤسسي بمعالجة العمليات الخاصة بإنشاء المحتوى ومراجعته واعتماده ونشره على شبكة الإنترنت. وتشتمل البيانات الرئيسية للمحتوى الموجود على شبكة الويب على أدوات الإنشاء والتأليف أو التكامل وإدارة وتصميم المدخلات وقالب العرض وإدارة إعادة استخدام المحتوى وقدرات النشر الفعالة.

• **أدوات التشارك في نظام إدارة المحتوى المؤسسي وأدوات الحوسبة الاجتماعية:** تمكن التقنيات المستخدمة في التعاون أو التشارك المستخدمين المستقلين، كالموظفين أو شركاء العمل، من أن يقوموا بسهولة بتشكيل فرق المشروع والحفاظ عليها، بغض النظر عن الموقع الجغرافي. إن هذه التقنيات وأدوات الحوسبة الاجتماعية تقوم بتسهيل العمل التعاوني وإنشاء المحتوى القائم على الفريق، واتخاذ القرار لكل من نظم تقنية المعلومات التقليدية والعدد المتزايد لعمليات حوسبة الشبكة الاجتماعية في المؤسسة. كما أن هناك حاجة إلى الاحتفاظ بسجلات مناسبة لهذه الأنشطة.

• **البحث وتحليلات المحتوى:** سواء كان بسبب الإستراتيجيات التسويقية أو الوصاية الحكومية أم غيرها من العوامل، فالمؤسسات بحاجة متزايدة للقيام بمراجعة وتحليل العديد من المعاملات الخاصة بأعمالها. فعلى الرغم من أننا نمتلك قاعدة بيانات قوية كأحد أدوات المساعدة، فإن عمليات إدارة المحتوى المؤسسي يمكن أن تساعد كثيراً في الإبقاء على نتائج هذه الأنشطة.

• **أدوات الاستمرارية والاحتفاظ:** يعد الإبقاء على الأعمال سارية ومستمرة أربعاً وعشرين ساعة في اليوم، وسبعة أيام في الأسبوع ٧/٢٤، أحد مهام التخطيط للاستمرارية، ونظراً لأن الوثائق الإلكترونية هذه الأيام تعد بمثابة شريان الحياة بالنسبة لمعظم المؤسسات، فإن إدارة المحتوى المؤسسي لديها تلعب دوراً هاماً في إدارة الاستمرارية. حيث تسمح

التقنيات الخاصة بإدارة المحتوى المؤسسي بإنشاء مستودعات مركزية يمكن أن تتواجد بها كل المعلومات الحيوية للشركة. وسوف تختلف طريقة التخزين اعتماداً على مدى أهمية المحتوى بالنسبة للشركة، وهي تتنوع من أشرطة النسخ الاحتياطي خارج الموقع إلى المواقع الإضافية والمواقع الانعكاسية (المرآوية) المفصلة جغرافياً والموجودة على شبكات طاقة مختلفة. كما يجب على المؤسسة أن تضع أوليات لعناصر المحتوى لديها لتحديد مدى السرعة اللازمة لاستعادة محتوى الوثيقة على شبكة الإنترنت حال حدوث كارثة، كما يلزم تحديد العمليات المحورية في أداء المهام والكيانات التي تعتمد عليها، على أن يلي ذلك إجراء تقييم تأثير الأعمال لتحديد أثر حدوث عرقلة لتلك العمليات أو فقدانها. لذا فوجود عمليات مناسبة وقوية لإدارة المحتوى المؤسسي يعد هنا من الأمور الضرورية.

- **وسائل لإشراك عملاء نظام إدارة المحتوى المؤسسي:** إن وجود الأدوات التي تسمح للمؤسسة وعمالها وغيرهم من أصحاب المصلحة باسترجاع جميع المستويات الخاصة بأنشطة التعاملات والوصول إليها بسهولة يجب أن يكون سمة رئيسية من سمات عمليات نظام إدارة المحتوى المؤسسي. هذا النوع من الأدوات يسمح لمركز خدمات العملاء بتوفير تواريخ عمليات الشراء بشكل سريع بدلاً من العودة إلى السجلات واسترجاعها.
- **إدارة الوثائق:** تساعد عمليات إدارة المحتوى المؤسسي هنا المنظمات على تحقيق إدارة أفضل للقيام بإنشاء ومراجعة واعتماد واستخدام الوثائق الإلكترونية. توفر إدارة الوثائق الميزات الرئيسية كالخدمات المكتبية وتوصيف الوثائق والبحث وتسجيل الدخول والخروج والتحكم في الإصدار وتاريخ التنقيح وأمن الوثائق.
- **روابط التشغيل البيئي للمؤسسة:** تحتاج المؤسسة عادة في هذه الأيام إلى تبادل البيانات والمعلومات بين وحداتها التشغيلية المختلفة وأصحاب المصالح الخارجيين. وعلى الرغم من أن النظم والتصميمات المختلفة قد تتسبب في وجود صعوبات، فإنه ينبغي أن تكون عمليات إدارة المحتوى المؤسسي مفتوحة ومرنة بما يكفي لبناء روابط تشغيل بيئي للنظم التي تغطي المؤسسة بكاملها ووحداتها التشغيلية.

• أدوات أمن إدارة المحتوى المؤسسي: يجب أن تقوم عمليات إدارة المحتوى المؤسسي بفرض قيود على عمليات الوصول إلى المحتوى أثناء إنشائها وكذلك إدارتها عند تسليمها. وينبغي أن تشمل هذه العمليات الأمنية على ما يلي:

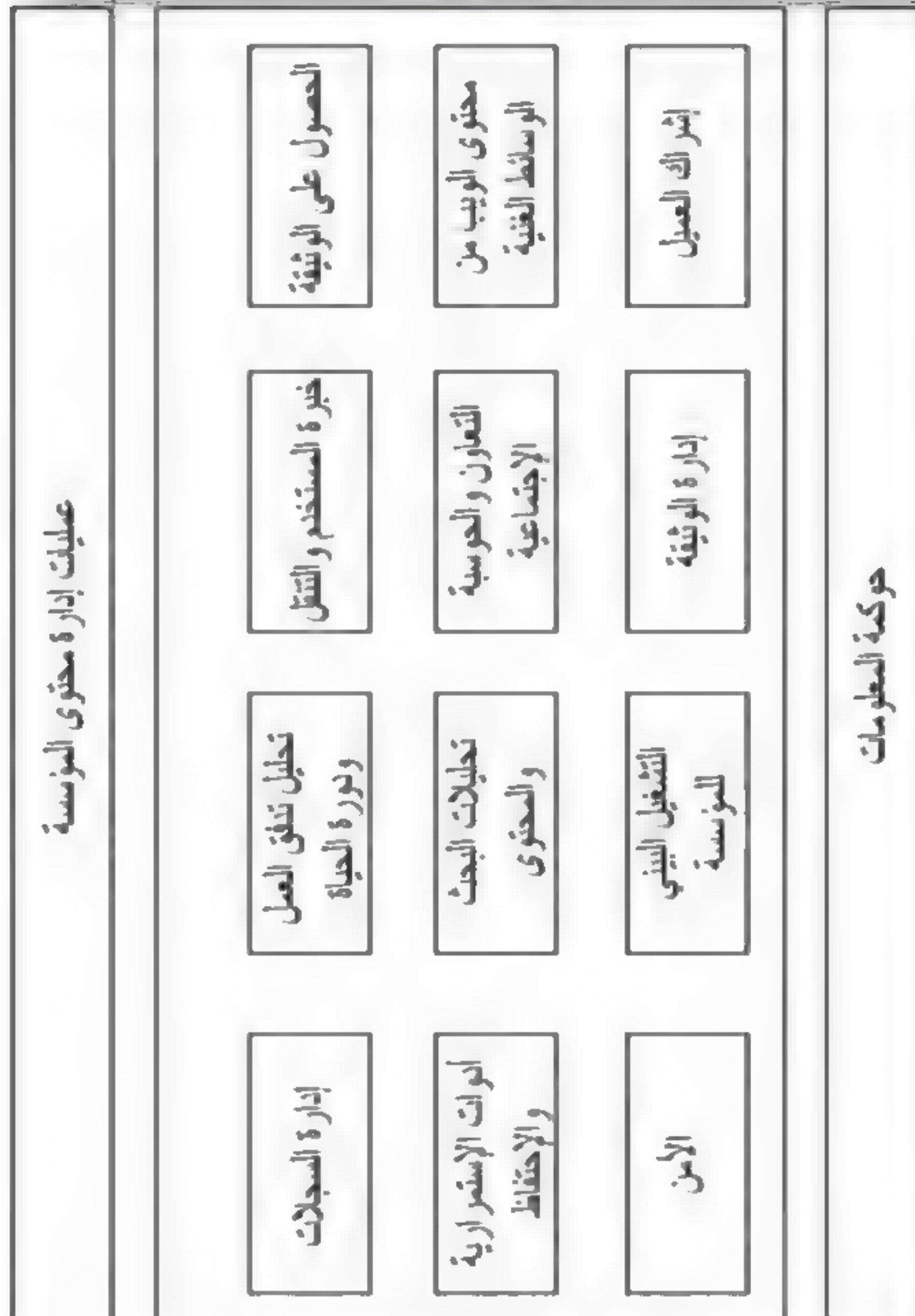
- إدارة الحقوق الرقمية: يجب أن تقوم عمليات إدارة المحتوى المؤسسي بمنع التوزيع غير المشروع للمحتوى المحمي بالحقوق عن طريق تقييد الوصول إلى المحتوى وصولاً (نزولاً) إلى مستوى الجملة وكذلك منح / تقييد الصلاحيات للتوجيه إلى المحتوى والوصول إليه.
- التوقيعات الرقمية: يجب أن تتأكد العمليات من هوية مرسل الوثيقة وسلامة الرسائل.

هناك عنصران آخران في إطار بنية نظام إدارة المحتوى المؤسسي الموضح في الشكل التوضيحي (١٨-١) لا يجب تجاهلهما. فالمربع أو الجزء العلوي من هذا المخطط عبارة عن مساحة يطلق عليها إدارة الامتثال. فالعنصر الأساسي في إستراتيجية الامتثال الناجح لنظام إدارة المحتوى هو الحاجة إلى الدمج بين فكرة الامتثال لنظام إدارة المحتوى والأعمال وألا يُنظر للامتثال هنا كما لو كان مشروعاً يمكن أن يبدأ و"ينتهي"، وعلى الرغم من أن الامتثال للوائح التنظيمية يعد أمراً شاقاً، فإنه يجب أن يُنظر إليه على أنه فرصة لتحسين العمليات المشتركة للأعمال، وليس فقط مجرد تكلفة مستمرة على الأعمال. إن هذا المستوى من الامتثال يختلف قليلاً عن مكون الامتثال - الحوكمة وإدارة المخاطر والامتثال - GRC الخاص بحوكمة تقنية المعلومات.

إن التأسيس السليم للمبادرة الخاصة بالامتثال سيعود بالفائدة على العديد من مجالات الخبرة في المؤسسة خصوصاً المجالات القانونية وتقنية المعلومات وإدارة السجلات، والتي تهدف جميعها إلى دعم الأهداف العامة للأعمال المؤسسية. ويجب أن تسهم معرفة ومرييات الأفراد العاملين في كل من هذه المجالات في تحقيق الفوائد المرجوة من البرنامج السليم للامتثال. وعلى الرغم من أن الامتثال لا يمثل دائماً مشكلة تقنية، فإن تقنية المعلومات، والنمو الهائل للمحتوى غير المركب، قد يسهمان في كشف محتوى الشركات. وقد يساعد الاستخدام السليم لأدوات إدارة المحتوى المؤسسي في الحد من التكلفة الإجمالية للامتثال بالنسبة للأعمال وفي تحسين حوكمة تقنية المعلومات بشكل عام، كما هو موضح في العنصر الموجود في أسفل الشكل التوضيحي (١٨-١).

شكل توضيحي (١٨-١)

معمارية إدارة محتوى المؤسسة ECM



خلق بيئة فعالة لنظام إدارة المحتوى المؤسسي في المؤسسة:

كما أشرنا في النقاشات التمهيدية لهذا الفصل، ليست إدارة المحتوى المؤسسي مجرد نظام واحد ولكنه أكثر من إستراتيجية للمؤسسة، فهو عبارة عن سلسلة من النظم والعمليات

لإدارة العديد من النماذج والصيغ التي تتعامل معها المؤسسة اليوم بشكل أفضل، بدءاً من الوثائق الورقية وصولاً إلى الملاحظات المنشورة على تويتر Twitter والرسوم الهندسية، وما هو أكثر من ذلك بكثير. وقد قامت بعض إدارات تقنية المعلومات في المؤسسة بوضع إستراتيجية خاصة بإدارة المحتوى المؤسسي، وربما تكون قد قامت بتطبيق ذلك النهج الخاص بتلك الإستراتيجية إلى حد كبير. ومن الممكن أن تكون بعض الإدارات الأخرى قد قامت بتطبيق بعض الأجزاء الفعالة في نظام إدارة المحتوى المؤسسي كنظام خدمة العملاء للتحقق من الطلبات، ولكن لا يزال لدى تلك الإدارات الوسائل التي تسلكها قبل إطلاق نظام لإدارة المحتوى المؤسسي بشكل كامل. ثم من الممكن أن يكون هناك بعض الشركات التي لم تتناول المفهوم بالشكل الصحيح ومن ثم استمرت في استخدام أساليبها التقليدية القائمة على التعامل مع الوثائق واحدة تلو الأخرى.

يمكن أن تكون العمليات الفعالة لإدارة المحتوى المؤسسي وسيلة جيدة جداً لتحسين حوكمة تقنية المعلومات في المؤسسة. الشكل التوضيحي (١٨-٢) يوضح بعض الشروط التي يجب على الإدارة مراعاتها عند اعتماد إستراتيجية خاصة بإدارة المحتوى المؤسسي. فإذا قامت المؤسسة بتحقيق واحد أو أكثر من تلك المتطلبات، ولاسيما إذا قامت بتلبية العديد منها بشكل مناسب، فمن الممكن أن تستفيد من عملية تحولها لاستخدام نظام إدارة المحتوى المؤسسي.

يتطلب التحول إلى استخدام نظام إدارة المحتوى المؤسسي شكلاً من أشكال الإستراتيجية في خطوة أولى. حيث تتضمن بعض الخيارات الخاصة بوضع إستراتيجية للتحول إلى استخدام نظام إدارة المحتوى المؤسسي على مستوى المؤسسة ما يلي:

- القيام بداية ببناء منصة جديدة لإدارة المحتوى المؤسسي في أماكن العمل، وذلك باستخدام إحدى العروض المقدمة من مقدمي خدمات المنصات الفردية لإدارة المحتوى المؤسسي.
- تهجير واستبدال جميع نظم إدارة المحتوى الموجود إلى منتج واحد جديد خاص بإدارة المحتوى والذي حصلنا عليه من قبل أحد الموردين الذي يعمل على مستوى المؤسسة.
- نقل أو تحويل كل نظم إدارة المحتوى الموجودة إلى المنتج الفردي الموجود الذي تم اختياره لإدارة المحتوى على مستوى المؤسسة والمقدم من قبل البائع.

شكل توضيحي (٢-١٨)

متطلبات المؤسسة التي تبرر الانتقال إلى نظام إدارة المحتوى المؤسسي

- الاحتفاظ الطويل الأجل بالسجلات أو المتطلبات.
- الاحتياجات اللوجستية لإدارة السجلات المادية واسترجاعها.
- الاحتياجات الخاصة بامتلاك المعلومات أو السجلات كبيرة الحجم.
- احتياجات التوافق مع معايير إدارة السجلات (على سبيل المثال، الحكومة الاتحادية أو الأيزو).
- البيئة اللازمة لمشروع إدارة ومعالجة القضايا والحالات.
- عمليات السجل أو المستند المهمة المدعومة بالتوقيع.
- إدارة الأصول الرقمية (الوسائط الغنية).
- إدارة التصميمات التقنية أو الضخمة الصياغة.
- متطلبات إدارة الأصول والمرافق.
- بوابات شبكة الإنترنت الخارجية / التي يتعامل معها العملاء.
- الحاجة للتعامل مع شريك خارجي لتقديم حماية الجدران النارية.
- تطبيقات لإدارة عمليات المهام الصعبة.
- المتطلبات أو الاحتياجات اللازمة لإدارة الطباعة / الإخراج / الإحالات.
- التكامل الوثيق مع نظم ERP / CRM / LOB.
- اتصالات النظم الواردة ذات القنوات المتعددة.
- متطلبات إدارة الحقوق الرقمية / للأصول ذات القيمة العالية.
- متطلبات تشفير البيانات التي على درجة عالية من الأمن.

• التعديل أو الاستبدال أو التحويل الانتقائي للعديد من النظم الإدارية/ المحلية المعمول بها حالياً حسب الحاجة.

• تركيب نظم إدارية جديدة متخصصة حسب الحاجة لتحقيق الأهداف المحلية.

• الانتقال إلى منصة نظام إدارة المحتوى المؤسسي القائمة على البيئة السحابية والمقدمة من قبل طرف ثالث.

ليس الهدف من هذا الفصل تقديم التفاصيل اللازمة لتطبيق إستراتيجية إدارة المحتوى على مستوى المؤسسة بواسطة استخدام العناصر التي تم وضعها، أو عن طريق التعامل مع أحد الباعة الرئيسيين مثل آي بي إم (IBM) أو إي إم سي (EMC) والذين بإمكانهم تقديم الإرشادات والأدوات اللازمة. تُقدم الأجزاء التالية من هذا الفصل وصفاً للعناصر الأساسية لكامل نظام إدارة المحتوى المؤسسي أو لسلسلة من العمليات. كما يجب أن تشمل الإدارة الفعالة للمحتوى على معظم هذه العناصر.

سمات نظام إدارة المحتوى المؤسسي: الأرشفة Archiving:

تضطر الأعمال هذه الأيام إلى التعاطي مع مجموعة كبيرة من مصادر البيانات المختلفة للشركات والإدارات. والتي تتضمن قواعد البيانات العلاقية، ومستودعات الوثائق، ومخازن البريد الإلكتروني، وخوادم الملفات. والأمر الذي يزيد من حجم التحدي الناجم عن إدارة هذه البيئة المعقدة لمصادر البيانات المختلفة هو المتطلبات المتعلقة بمقتنيات وممتلكات الشركات والتشريعات التنظيمية وحوكمة المعلومات والتفويضات للحد من التكلفة التشغيلية من خلال البائع وتعزيز البنية التحتية. وتحتاج المؤسسة إلى مستودعات خاصة بأرشفة وثائق نظام إدارة المحتوى المؤسسي، وذلك لتخزين تلك الوثائق التي تكون غالباً ملايين من البيانات والوثائق والصور، وغيرها من الوثائق التي تخص العملاء. ويجب أن يشمل هذا الأرشفة على جميع الوثائق الفردية الخاصة بالاستكشاف والتحقق من سلامة وصحة المحتوى وتنظيم العمليات التخزينية والاسترجاع والتوزيع والتوصيل.

ترتبط الفهارس الخاصة عادة بأرشفة وثائق نظام إدارة المحتوى المؤسسي بمحتوى المستند عند إنشاء ذلك المحتوى وذلك من خلال استخدام محركات التركيب، أو أثناء تحميلها في الأرشفة. تصميم الفهرس هنا مهم، فبمجرد وضع الوثائق في الأرشفة سيكون من الصعب جداً نمو أو زيادة تلك الفهارس لكي تلبي الاحتياجات المتغيرة للأعمال أو الاحتياجات الخاصة بالعملاء طبقاً لوجهات النظر المختلفة لهم.

وعلى الرغم من أن مشروع الأرشفة الخاصة بإدارة المحتوى المؤسسي قد يكون "مشروعاً مرعباً"، فإنه يوفر فرصة لتوضيح مسائل مثل رقم الحساب ومعايير التسمية التي قد تكون فريدة داخل مؤسسة واحدة ولكن تتكرر عبر السجلات المحفوظة لدى الشركة. فبالإضافة

إلى إطلاق مجموعة من العمليات الخاصة بإدارة المحتوى المؤسسي، يمكن للأرشفة أن تعود على المؤسسة بفوائد فورية - وطويلة الأجل.

سمات نظام إدارة المحتوى المؤسسي: عمليات التصنيف Classification Processes:

تعمل عمليات التصنيف الخاصة بوثائق نظام إدارة المحتوى المؤسسي على أتمته تنظيم المحتويات غير المركبة، وذلك من خلال تحليل النص الكامل لوثائق ورسائل البريد الإلكتروني. ومن خلال تصنيف المحتوى، بإمكان تقنية المعلومات أن تقوم بتسريع عمليات الوصول إلى المحتوى أو تقليل الوقت اللازم للوصول إليه، وذلك للحصول على القيمة المرجوة من الاستثمارات المتعلقة بنظام إدارة المحتوى المؤسسي كأرشفة المحتوى أو إدارة السجلات الإلكترونية. ويجب أن تسمح عمليات التصنيف بالتالي:

- تقديم أعلى عوائد الاستثمار من العملية عن طريق تحرير المستخدمين النهائيين من عبء المهام اليدوية دون المخاطرة بتعارض المشاركة - في حين أنه يتم تصنيف كميات كبيرة من المحتوى بدقة.
- تصفية أرشيف الوثائق من رسائل البريد الإلكتروني والوثائق ذات القيمة المحدودة بالنسبة للأعمال.
- تنظيم محتوى الوثائق بمنطق ثابت وموثوق به وقابل للتدقيق.
- أكثر استعداداً للتكيف مع التغييرات في السياسات والفئات من خلال دمج التغذية الراجعة للمستخدم في الوقت الحقيقي.
- إنشاء تصنيفات عالية الدقة للوثائق من خلال الجمع بين أساليب متعددة للتصنيف مثل:
 - قواعد الكلمات المفتاحية والتطابق التقريبي.
 - استخراج النمط.
 - الأساليب القائمة على السياق الدقيق للغاية الخاصة بـ "التعلم من خلال قدوة".

إن عملية تحليلات المحتوى هي العنصر الرئيسي في عمليات تصنيف وثائق نظام إدارة المحتوى المؤسسي، وهي عملية متقدمة للبحث والتحليلات تُمكن من اتخاذ قرارات أفضل اعتماداً على محتوى المؤسسة بغض النظر عن مصدر ذلك المحتوى أو شكله. بإمكان الحلول الخاصة بعملية تحليلات المحتوى فهم معنى وسياق لغة الإنسان وتقوم بسرعة بمعالجة المعلومات لتحسين البحث الذي تحركه المعرفة وإظهار رؤى جديدة من محتوى المؤسسة الخاصة بك.

وما هو أكثر تطوراً من ذلك استخدام تقنيات أحدث لمعالجة اللغات الطبيعية مثل تقنية (IBM Watson DeepQA)، وذلك عند إجراء عمليات تحليل المحتوى، وهذه التقنية عبارة عن آلة متطورة تعمل بنظام الرد على الأسئلة. إن كمية كبيرة من المعلومات التي تم إنشاؤها واستخدامها من قبل المؤسسة عبارة محتوى غير مركب، والذي ينمو عادةً بمعدل ضعف معدل البيانات المركبة. إن تسخير واستخدام هذه المعلومات غير المركبة وشبه المركبة قد يساعد المنظمة للعمل بطريقة أذكى ويخدم العملاء بشكل أفضل ويتحكم في التكاليف ويخطط للمستقبل.

سمات نظام إدارة المحتوى المؤسسي: التخلص من الوثائق وإدارة الحوكمة:

يجب أن تكون عملية التخلص من الوثائق وإدارة الحوكمة جزءاً لا يتجزأ من عمليات إدارة المحتوى المؤسسي في المؤسسة. إذ تساعد هذه العملية المؤسسة على الوفاء بالتزاماتها للحصول على المعلومات وإدارتها على أساس القيمة والتخلص من المعلومات العديمة القيمة أو الالتزامات في أقرب فرصة ممكنة. فقد تساعد العملية المُحَكَّمة على التخلص من البيانات التي لم تعد مستخدمة في الحد بشكل كبير من حجم المعلومات ومن التكاليف الناجمة عن استخدام تقنية المعلومات. فمن خلال الحلول المناسبة للتخلص من البيانات وإدارة الحوكمة يمكن لتقنية المعلومات أن تقوم بإدارة المعلومات وفقاً لقيمة أعمالها أو التزاماتها القانونية وتقوم بالتخلص من المعلومات الأخرى.

إن العنصر الأساسي في عمليات التخلص من الوثائق هو أنه يجب على إدارة المؤسسة وإدارة تقنية المعلومات الحصول على رؤية واضحة للوثيقة فيما يخص أنه يجب على إدارة المؤسسة وإدارة تقنية المعلومات الوصول إلى رؤية لكل من وثائق الالتزامات القانونية -

كالجداول القانونية لإدراج الوثائق والاحتفاظ بها - والقيمة التجارية لمعلومات محددة مرتبطة بأحد الأصول أو بهوية أحد الموظفين. كما يجب أن يكون لدى عمليات إدارة المحتوى المؤسسي أهداف للقيام بالنقل الفوري للمتطلبات والحقائق بين كل من قسم تقنية المعلومات والسجلات والكادر القانوني للمؤسسة، وذلك من خلال التبليغ التلقائي لمهام البنود والإشعارات والتنبيهات وعمليات البحث المبسطة في الالتزامات القانونية.

يجب على المنشأة أن تقوم بالتخلص المبرر من الوثائق، وذلك من خلال إجراء عمليات دقيقة لجرد البيانات بهدف التخلص من المعلومات المخزنة الزائدة عن الحاجة. فمن خلال تمكين تقنية المعلومات لإجراء عمليات تحديد النسخ المكررة البيانات نفسها والبيانات القديمة التي لم يعد لها أي قيمة تجارية أو عليها التزامات قانونية وكذلك النظم المكررة، فإنه يمكن لعمليات إدارة المحتوى أن تُمكن الشركة من الاحتفاظ فقط بالبيانات التي لها قيمة محتملة.

وتستطيع العمليات المناسبة لإدارة المحتوى المؤسسي أن تمنع تراكم البيانات غير الضرورية في المستقبل. فعندما تقوم المؤسسة بالتخلص المبرر من المعلومات التي يمكن الاستغناء عنها فإن ذلك يمكنه أن يقضي على مخاطرة ترتبط بتقنية المعلومات تُعرف بـ"ادخار كل شيء"، ومن ثم زيادة الكتلة القابلة للاستكشاف. كما أنه يحمي المؤسسة من الانشغال بممارسات تخلص مفرطة وغير مناسبة بسبب إجراءاتها عمليات غير مناسبة وإهدارها لفترات حفظ لم تكون مطلوبة.

هناك مئات الحلول الأخرى لممارسة إدارة الوثائق المكتبية مثل التصوير والتطبيقات الهندسية وإدارة محتوى الويب والمحتوى القائم على XML وتطبيقات نشر الوثائق. فإدارة الوثائق تتيح آليات البحث والوصول إلى الوثائق الموجودة في تلك النظم في جميع أنحاء المنظمة في الوقت الذي تتبنى فيه المعايير الصناعية التي تساعد على التكامل مع عمليات الأعمال الأخرى. وتقوم إدارة الوثائق بزيادة حجم البنية التحتية الخاصة بنظام إدارة المحتوى المؤسسي لتشمل وثائق العمل التي تم إنشاؤها بشكل فردي أو عن طريق العمليات التعاونية.

هناك العديد من التقنيات والحلول المتاحة التي يقوم المورد بتوفيرها هذه الأيام في إدارة المحتوى المؤسسي، إلا أن نظام إدارة المحتوى الأكثر أهمية هو الذي يمتلك خطة إستراتيجية مستمرة ومتطورة لزيادة الكيفية التي يمكن من خلالها استخدام المحتوى. قد تكون العمليات المتعلقة بمعلومات نظام إدارة المحتوى المؤسسي بمثابة نقطة انطلاق للمؤسسة للقيام بمراجعة وإنشاء دورة حياة مشتركة لمحتوى المعلومات. وكنقطة بداية لحوكمة تقنية المعلومات، يجب على المؤسسة رسم خريطة لنظمها وعملياتها الحالية لتحديد أوجه التداخل ومجالات التحسين للتطبيقات والإستراتيجيات التي تقوم بتطويرها. وقد تكون المعلومات المٌجمعة بمثابة مؤشر فقط على درجة التعقيد المتأصلة في أي عملية تدير محتوى منظمة ما. وينبغي أن تتمثل الخطوة التالية في مناسبة الأدوات التقنية لتلبية احتياجات الأعمال. ويمكن للتقنية أن تضمن انسيابية إدارة المحتوى، لكن الإستراتيجية الأساسية يجب أن تأتي أولاً.

الفصل التاسع عشر

دور التدقيق الداخلي في الحوكمة

من المعلوم أن مهنة التدقيق الداخلي ليست جديدة وإنما هي موجودة منذ القدم. فقد اكتشف علماء الآثار أن الكتبة في بلاد ما بين النهرين^(*) قد استخدموا سجلات محاسبية دقيقة من ألواح الطين منذ ما يقرب من ٣٠٠٠ سنة قبل الميلاد حيث كانت تحتوي تلك السجلات على مؤشرات ونقاط وعلامات تحديد، وهو الأمر الذي يدل على وجود وظيفة التدقيق في ذلك الوقت. ودون شك فقد تطورت مهنة التدقيق على مدى آلاف السنين، ونقوم اليوم عادة بتصنيف معظم مدققي الأعمال إما إلى مدققين خارجيين أو مدققين داخليين. حيث يتم اعتماد المدقق الخارجي من قبل هيئة تنظيمية ليقوم بزيارة المؤسسة أو المنشأة لمراجعة أعمالها والقيام بإعداد تقرير مستقل بنتائج هذه المراجعة. ففي الولايات المتحدة يكون المدققون الخارجيون عادة هم المحاسبين القانونيين، الذين يحملون تراخيص من الولاية ويتبعون المعايير الخاصة بالمعهد الأمريكي للمحاسبين القانونيين (www.aicpa.org). كما يوجد هناك أيضاً أنواع أخرى من المدققين الخارجيين الذين يعملون في مجالات مثل من يقومون بمراجعة مدى مطابقة الأجهزة الخاصة بالمعدات الطبية للمعايير أو مراجعة معدلات مشاهدي التلفاز أو غيرها من التقييمات في مجالات حكومية متعددة.

يكون مجال التدقيق الداخلي غالباً أكثر اتساعاً وأهمية من مجال التدقيق الخارجي. وكون المدقق الداخلي من موظفي أو أعضاء المؤسسة، فإنه يقوم وبشكل مستقل بمراجعة وتقييم العمليات التشغيلية في العديد من المجالات المختلفة، مثل إجراءات الرقابة الداخلية للمكاتب المحاسبية أو العمليات الخاصة بالجودة الصناعية. ويقوم معظم المدققين الداخليين باتباع معايير رفيعة المستوى تم وضعها من قبل المنظمة المهنية التي يتبعونها، وهي معهد المدققين الداخليين (IIA، www.theiia.org)، غير أنه يوجد اليوم كثير من الممارسات والأساليب المختلفة الأخرى في التدقيق الداخلي نتيجة لطبيعته العالمية وكثرة أنواع أنشطة التدقيق.

(*) بلاد العراق قديماً (المترجم).

يتخصص بعض المدققين الداخليين في مراجعة الضوابط المالية الداخلية للمؤسسات، في حين يركز البعض الآخر على عمليات الأعمال أو المسائل التشغيلية. وعلى الرغم من أن جميع المدققين الداخليين اليوم يجب أن يكون لديهم بعض المعرفة عن الضوابط الداخلية المتعلقة بتقنية المعلومات، فإن هناك أيضاً تخصصاً مهنيّاً قوياً يعرف باسم مدقق تقنية المعلومات. وقد تم الحديث عن هؤلاء المهنيين في الفصل الخامس من هذا الكتاب باعتبارهم الموارد الرئيسية لتطوير وتنفيذ عمليات قوية وفعالة لحوكمة تقنية المعلومات.

يستعرض هذا الفصل أهمية التدقيق الداخلي وتدقيق تقنية المعلومات في وضع عمليات فعالة لحوكمة تقنية المعلومات. وسوف نستعرض بإيجاز المعايير والأنشطة المهنية الخاصة بالتدقيق الداخلي والضرورية لإيجاد ممارسات جيدة لحوكمة تقنية المعلومات. وعلى الرغم من أن إدارة التدقيق الداخلي تعد إدارة منفصلة ومستقلة داخل المؤسسة، فإن التقارير الصادرة عنها تُقدّم فقط للجنة التدقيق التابعة لمجلس إدارة المؤسسة، لذا يجب على المديرين التنفيذيين فهم الأدوار المنوطة بهم والعمل معهم بهدف تحسين العمليات الخاصة بحوكمة تقنية المعلومات.

تاريخ التدقيق الداخلي ومعلومات أساسية عنه:

يمكن لكبار المديرين التنفيذيين فهم التدقيق الداخلي ومجالاته المعرفية الأساسية على نحو أفضل من خلال معرفتهم لبعض المعلومات عن المنظمة المهنية للمدققين الداخليين، IIA، ومعاييرها المهنية المنشورة. وقد قامت تلك المنظمة المهنية بتعريف التدقيق الداخلي على النحو التالي:

"التدقيق الداخلي هو وظيفة تقييم مستقلة مصممة داخل المنظمة لفحص وتقييم أنشطتها باعتبارها خدمة للمنظمة."

سيكون هذا التعريف أكثر وضوحاً عندما نركز على مصطلحاته الأساسية. حيث يشير التدقيق إلى مجموعة متنوعة من الأفكار التي يمكن أن يُنظر إليها من زاوية ضيقة للغاية، مثل التحقق من الدقة الحسابية أو الوجود الفعلي للسجلات المحاسبية، أو على نطاق أوسع كالمراجعات والتقييمات التي تتم على العديد من المستويات التنظيمية. سيتم استخدام مصطلح التدقيق طيلة هذا الفصل ليشمل هذه المجموعة المتنوعة من مستويات الخدمة،

التي تمتد من الفحص التفصيلي وحتى الوصول إلى التقييمات العالية المستوى. أما مصطلح الداخلي فيقصد به أن العمل يتم داخل المؤسسة، بواسطة الموظفين العاملين فيها، بعكس المدققين الخارجيين الذين يتم تنفيذ أعمالهم بواسطة محاسبين قانونيين أو أطراف أخرى من خارج المؤسسة، كالمنظمات أو الجهات الرقابية الحكومية، التي لا تعتبر جزءاً من المؤسسة.

يشتمل الجزء المتبقي من هذا التعريف الخاص بالمنظمة المهنية للمدققين الداخليين IIA والخاص بالتدقيق الداخلي على مصطلحات أخرى هامة تنطبق على هذه المهنة وهي:

- مستقلة: هو المصطلح الذي يشير إلى أن التدقيق الداخلي خال من أية قيود يمكن أن تحد بشكل كبير من نطاق وفاعلية أي عملية مراجعة يقوم بها المدقق الداخلي أو تؤثر في التقارير التي يتم إعدادها بعد ذلك بشأن المحصلة النهائية الخاصة بالنتائج والاستنتاجات.
- التقييم: هو مصطلح يؤكد ضرورة إجراء التقييم الذي يعد بمثابة قوة الدفع للمدققين الداخليين عند قيامهم بوضع استنتاجاتهم.
- مصممة: هو مصطلح يؤكد أن التدقيق الداخلي عبارة عن وظيفة رسمية محددة داخل المؤسسة الحديثة.
- فحص وتقييم: مصطلحان يصفان الأدوار النشطة التي يقوم بها المدققون الداخليون، بداية بالاستفسارات الخاصة بتقصي الحقائق ثم بالتقييمات التحكيمية النزيهة.
- أنشطتها: هو مصطلح يؤكد النطاق الواسع لولاية أو سلطة الأعمال الخاصة بالتدقيق الداخلي والذي يسري على جميع أنشطة المؤسسة الحديثة.
- الخدمة: مصطلح يشير إلى أن المساعدة ومد يد العون إلى لجنة التدقيق والإدارة وغيرهم من أعضاء المؤسسة هي الغاية الحقيقية النهائية من جميع أعمال التدقيق الداخلي.
- المنظمة: مصطلح يؤكد أن النطاق الإجمالي لخدمة التدقيق الداخلي يشمل المؤسسة بأكملها، متضمناً ذلك جميع الموظفين ومجلس الإدارة ولجنة التدقيق والمساهمين وغيرهم من أصحاب المصالح.

كما يجب الاعتراف أيضاً بأن إدارة التدقيق الداخلي تعد بمثابة هيئة رقابية تنظيمية داخل المؤسسة تعمل من خلال قياس وتقييم فاعلية الضوابط الأخرى. فالمدققون الداخليون الذين يقومون بأداء أعمالهم بفاعلية وكفاءة يُصبحون خبراء في عمل أفضل التصاميم والتطبيقات الممكنة لجميع أنواع الضوابط والممارسات المفضلة. وتتضمن هذه الخبرة فهم أوجه الترابط بين الضوابط المختلفة وأفضل تكامل ممكن فيما بينها داخل النظام الكلي للرقابة الداخلية. وبذلك تعد الرقابة الداخلية بمثابة الباب الذي من خلاله يأتي المدققون الداخليون لدراسة وتقييم جميع أنشطة المنظمة وتوفير أقصى قدر ممكن من الخدمات للمؤسسة. لا يمكن التوقع بأن يكون المدققون الداخليون متساوين - بغض النظر عن كثرتهم - في الخبرات الفنية والتشغيلية الخاصة بالعديد من الأنشطة المختلفة للمؤسسة. لكن ومع ذلك، يمكن للمدققين الداخليين مساعدة هؤلاء الأفراد المسؤولين في تحقيق نتائج أكثر فاعلية من خلال تقييم الضوابط القائمة وتوفير أساس للمساعدة على تحسين تلك الضوابط وكذلك الممارسات الخاصة بحوكمة تقنية المعلومات ذات الصلة.

بعض المعلومات الأساسية عن دور التدقيق الداخلي قد تكون ذات فائدة. فعلى الرغم من الأصول التاريخية القديمة للتدقيق الداخلي، فإنه لم يتم إدراك أو الاعتراف بمدى أهميته من قبل العديد من المؤسسات ومدققها الخارجيين حتى ثلاثينيات القرن الماضي. فقد كان السبب الرئيسي للاهتمام بمهنة التدقيق الداخلي والاعتراف به يعود في المقام الأول إلى إنشاء هيئة الأوراق المالية والبورصة الأمريكية (SEC) في عام ١٩٣٤ وتغير أهداف وتقنيات التدقيق الخارجي في ذلك الوقت. وفي هذا الوقت تماماً، تعرضت الولايات المتحدة وبقيّة دول العالم لكساد depression اقتصادي كبير بكل المقاييس، والذي كان أكثر شدة من الركود recession العالمي الكبير الذي بدأ في عام ٢٠٠٨. وفي إجراء تشريعي تصحيحي، طالبت هيئة الأوراق المالية والبورصة الأمريكية (SEC) المؤسسات المسجلة بضرورة تقديم بيانات مالية معتمدة من مدققي حسابات مستقلين. كما دفع هذا المطلب أيضاً الشركات إلى القيام بإنشاء إدارات التدقيق الداخلي، ولكن مع الحفاظ على الهدف الرئيسي في مساعدة مدققيها المستقلين. حيث قام المدققون الماليون الخارجيون وقتها بالتركيز على إبداء آرائهم حول نزاهة القوائم المالية للمؤسسة بدلاً من التركيز على كشف نقاط الضعف الموجودة في الرقابة الداخلية. وقد حثت قواعد هيئة الأوراق المالية والبورصة الأمريكية

(SEC) على التدقيق القائم على عينة محدودة من المعاملات، إلى جانب المزيد من الاعتماد على إجراءات الرقابة الداخلية.

وقد كان المدققون الداخليون في ذلك الوقت معنيين في المقام الأول بفحص السجلات المحاسبية والكشف عن الأخطاء والمخالفات المالية. وكانوا في كثير من الأحيان أكثر قليلاً من مساعدين لمدققي الحسابات الخارجيين المستقلين، والمكلفين بتنفيذ التسويات المحاسبية الروتينية أو بمثابة أفراد للدعم المكتبي. وقد استمرت آثار هذا التعريف القديم للتدقيق الداخلي في بعض الأماكن حتى أوائل السبعينيات من القرن الماضي. على سبيل المثال، حتى سبعينيات القرن الماضي كان "المدققون" العاملون في العديد من المنظمات التي تمارس عمليات البيع بالتجزئة هم الأشخاص الذين يقومون بعد النقدية وترصيد آلات تسجيل النقدية (تذكر تلك؟) في نهاية كل يوم عمل.

وعلى الرغم من أنه هناك أصواتاً أخرى تطالب بضرورة عمل شيء لتحسين إمكانيات المدققين الخارجيين والاستفادة منها بشكل أفضل، فإن هناك أموراً قد بدأت بالفعل بعد أن أتم فيكتور ز. برينك Victor Z. Brink أطروحته الجامعية عن التدقيق الداخلي قبل الخروج للخدمة في الحرب العالمية الثانية. وبعد انتهاء الحرب، عاد برينك لتنظيم ورئاسة التدقيق الداخلي لشركة فورد موتور (Ford Motor)، وقد نُشرت أطروحته الجامعية في الطبعة الأولى من الكتاب المرجعي القياسي المتاح الآن عن هذا الموضوع، التدقيق الداخلي الحديث^(١) (Modern Internal Auditing).

وقد انطلق معهد المدققين الداخليين (IIA) في الوقت نفسه تقريباً، في عام ١٩٤١، من خلال تأسيس الفرع الأول له في نيويورك، وسرعان ما تبعه إنشاء فرع آخر في شيكاغو. وقد تم تشكيل المنظمة من قبل الأشخاص الذين تم منحهم لقب "مدقق داخلي" من قبل مؤسساتهم، والذين يريدون تبادل الخبرات والمعارف المكتسبة مع الآخرين في هذا المجال المهني الجديد. وبذلك تمت عملية ولادة هذه المهنة وارتفاع مكانتها وأهميتها منذ ذلك الحين.

كانت مهنة التدقيق الداخلي الحديث في أربعينيات القرن الماضي تتطلب مجموعة من المهارات المهنية المختلفة تماماً عما هي عليه اليوم. على سبيل المثال، لم تكن بعض الأجهزة الإلكترونية ميكانيكية وأنشطة مختبرات الأبحاث ونظم الحاسب الرقمية موجودة في

ذلك الوقت. هذا بالإضافة إلى عدم حاجة المؤسسات في ذلك الوقت إلى مبرمجي الحاسب الآلي حتى بدأت تصبح بعض آلات الجدولة البدائية مفيدة في حفظ السجلات وغيرها من المهام الحسابية والمحاسبية. وبالمثل، كانت مؤسسات الاتصالات الهاتفية بدائية جداً، فقد كان يقوم مشغلو لوحة التوزيع (المقسم) بتحويل جميع المكالمات الواردة إلى عدد محدود من الهواتف المكتبية. أما اليوم، فلدينا بالطبع موارد لتقنية المعلومات ترتبط جميعها من خلال الشبكة الإلكترونية الضخمة للإنترنت المكونة من الاتصالات السلكية واللاسلكية في كل أنحاء العالم. وقد أدى التعقيد المتزايد للأعمال وغيرها في المؤسسات الحديثة إلى الحاجة إلى مدققين داخليين ليصبحوا متخصصين أكثر من أي وقت مضى في مختلف ضوابط الأعمال. لقد لعب هؤلاء المدققون الداخليون الأوائل في كثير من الأحيان دوراً محدوداً جداً في المؤسسات التابعة لها، في ظل مسؤولياتهم المحدودة نسبياً من مجموع الطيف الإداري. فالمدقق الداخلي الأول كان يُنظر إليه غالباً على أنه مراجع للسجلات المالية وأنه ضابط شرطة أكثر من كونه زميلاً في العمل. في بعض المؤسسات، كان لدى المدققين الداخليين مسؤوليات كبيرة في تسوية الشيكات الملغاة للمرتبات مع البيانات المصرفية أو مراجعة الحسابات الموجودة في المستندات النظامية للأعمال.

ومع مرور الوقت، ازداد حجم وشدة تعقيد العمليات التشغيلية في العديد من مؤسسات الأعمال، الأمر الذي استحدث مشاكل إدارية وضغوطاً جديدة على الإدارة العليا. وقد كانت ردة الفعل الطبيعية لذلك، هو إدراك العديد من كبار المديرين أن هناك احتمالات لتحسين الاستفادة من المدققين الداخليين. كان هناك بالفعل أفراد تم تعيينهم في وظيفة التدقيق الداخلي للمؤسسة، ويبدو أنه كان هناك سبب وجيه للحصول على قيمة أكبر من هؤلاء الأفراد مع زيادة طفيفة نسبياً في التكلفة.

وفي الوقت نفسه، أدرك المدققون الداخليون هذه الفرص، وقاموا باستحداث العديد من أنواع الخدمات الجديدة. وبذلك أخذ المدققون الداخليون على عاتقهم تدريباً مسؤوليات أكبر وأكثر تركيزاً على الإدارة في أعمالهم. ولأن التدقيق الداخلي كان في البداية موجهاً نحو المحاسبة إلى حد كبير، فقد كان الشعور بهذا الاتجاه التصاعدي بداية في مجالات المحاسبة والرقابة المالية. فبدلاً من مجرد التبليغ عن المخالفات المحاسبية ذات الصلة - مثل بعض

الوثائق التي تخلص من توقيع المشرف - بدأ المدققون الداخليون بالاستفسار عن عمليات الرقابة الشاملة التي هم بصدد مراجعتها. ومن ثم، بدأ عمل تقييم التدقيق الداخلي يمتد ليشمل العديد من المجالات غير المالية في المؤسسة.

وقد تسببت قواعد ومبادرات الأعمال الجديدة في الولايات المتحدة، مثل إطار الرقابة الداخلية (COSO)، الذي تم التحديث عنه في الفصل الرابع من هذا الكتاب، أو متطلبات قانون ساربنز أوكسلي (SOX)، الموضحة في الفصل الثاني من هذا الكتاب، في الزيادة المستمرة للحاجة إلى خدمات المدققين الداخليين. وبالإضافة إلى ذلك، فإن بعض المؤثرات البيئية الحديثة قد أوجدت احتياجات جديدة في مجالات مثل الحماية من المخاطر الصناعية وتقديم الدعم لبرامج مراقبة الجودة ومستويات مختلفة لمسؤوليات العمل، متضمناً ذلك المعايير الأخلاقية. هذه الحاجة إلى المعايير الأخلاقية تشمل معايير أعلى لحوكمة الشركات، وزيادة مشاركة مجالس الإدارة، ولجان التدقيق التابعة لها، ودوراً أكثر نشاطاً لأصحاب المصالح، وقدراً أكبر من الاستقلالية للمحاسب القانوني الخارجي.

أما اليوم، فقد توسعت أنشطة التدقيق الداخلي لتصل إلى جميع المجالات التشغيلية للمؤسسة وقد حازت لها مكاناً يحظى بالتقدير والاحترام على أنه جزء من أعمال ومجهودات الإدارة العليا. إن المدقق الداخلي اليوم يخدم وبشكل رسمي وفعال لجنة التدقيق التابعة لمجلس الإدارة، وإن مدير التدقيق الداخلي (CAE) اليوم لديه مستوى مباشر وفعال للتواصل مع تلك اللجنة نفسها الخاصة بالتدقيق، وإن هذا الوضع العام يعكس تقدماً كبيراً في نطاق تغطية التدقيق الداخلي ومستوى الخدمة لجميع مجالات المؤسسة. إن مهنة التدقيق الداخلي نفسها، من خلال تنميتها الذاتية وتطبيقها كما ينبغي، أسهمت في تحقيق هذا التقدم، وتمهيد الطريق لاستمرار الاتجاه التصاعدي لها. فهي الآن تعد مكوناً هاماً من مكونات العمليات الفعالة لحوكمة تقنية المعلومات.

التدقيق الداخلي ومدقق تقنية المعلومات:

لقد تحدثنا عن تطور كل من مهنة التدقيق الداخلي ومعهد المدققين الداخليين IIA كذلك، وهو المنظمة المهنية العالمية للتدقيق الداخلي. وعلى الرغم من أنه يجب على أي منظمة مهنية أن تقوم بتقييم أو تقدير احتياجات أعضائها في ضوء الظروف المتغيرة، فإن

من الممكن أن تكون هذه التغيرات في بعض الأحيان بطيئة بعض الشيء. أصابت تلك التغيرات معهد المدققين الداخليين (IIA) في غضون فترة النمو الهائل في نظم وعمليات تقنية المعلومات، والذي ربما يكون قد بدأ في أوائل السبعينيات من القرن الماضي. قد أدرك في ذلك الوقت عدد كبير ومتزايد من المدققين الداخليين أن تلك النظم والعمليات الجديدة الخاصة بتقنية المعلومات قد قدمت مجموعة واسعة من القضايا الجديدة للرقابة الداخلية، إلا أن المنظمة المهنية للتدقيق الداخلي التابعين لها لم تقدم الإرشادات أو الدعم الفني الكافي.

تم تشكيل المنظمة المهنية الجديدة، التي سميت بعد ذلك بجمعية مدققي معالجة البيانات الإلكترونية EDP Auditors Association، لدعم هؤلاء العاملين الجدد بالتدقيق الداخلي. ويرمز الاختصار EDP إلى معالجة البيانات الإلكترونية (Electronic Data Processing)، وهو أحد المصطلحات القديمة لنظم وعمليات تقنية المعلومات. ويُعرف هؤلاء المهنيون اليوم بأنهم مدققو تقنية المعلومات كما يطلق على المنظمة المهنية الرئيسية التابعين لها الآن اسم جمعية ضبط وتدقيق نظم المعلومات (Information Systems Audit and Control Association)، وهي منظمة مهنية هامة في مجال حوكمة تقنية المعلومات وقد تقدم ذكرها للمرة الأولى في الفصل الخامس من هذا الكتاب. يكون مدققو تقنية المعلومات غالباً متخصصين في الإدارات التقليدية للتدقيق الداخلي، ولكن يرتبطون كثيراً بشركات المحاسبة القانونية الرئيسية أو العمل كذلك بصفة مستشارين خصوصيين. ولهم دور هام جداً في وضع ومتابعة العمليات الفعالة لحوكمة تقنية المعلومات في المؤسسة.

يتعين على كبار مديري الأعمال فهم أدوار ومسؤوليات المدققين الداخليين فيما يخص حوكمة تقنية المعلومات في مؤسساتهم، مع إيلاء المزيد من الاهتمام بأخصائيي تدقيق تقنية المعلومات التابعين لها. فبالإضافة إلى الدور الذي يلعبه التدقيق الداخلي في تقديم التقارير إلى لجنة التدقيق التابعة لمجلس الإدارة، له دور ووظيفة خاصة جداً في المؤسسة. فهو بشكل عام يعمل بصفته نوعاً من أنواع الوظائف التعاونية، فهو يقوم بوضع الجدول الزمني والأنشطة الخاصة به غير أنه يدعم الإدارة العليا من خلال المراجعات والأنشطة والتقييمات. وستحدث الأقسام التالية عن بعض المسؤوليات الهامة للتدقيق الداخلي في حوكمة تقنية المعلومات المؤسسية.

أنشطة التدقيق الداخلي ومسئوليته المرتبطة بحوكمة تقنية المعلومات:

"كن حذراً، فالمدققون قادمون!" لقد شاع استخدام هذا النوع من التحذيرات في الماضي القريب عندما كانت إدارة التدقيق الداخلي تُخَطِر مدير المؤسسة بأنهم قاموا بإعداد جدول زمني لمراجعة أحد التطبيقات أو العمليات الخاصة بتقنية المعلومات بشكل عام أو بعض المجالات الأخرى ذات الاهتمام. وقد كانت ردة الفعل الطبيعية وقتها لصاحب عمليات تقنية المعلومات هي أن يقول بأن عمليات التدقيق المخطط لها قد تمت جدولتها في "الوقت غير المناسب" وذلك للعديد من الأسباب. ومع ذلك، كان موعد التدقيق الداخلي المخطط له قد تم تحديده قريباً، وأن التدقيق الداخلي سيقوم بإجراء المراجعات الخاصة بهم، وسيتم إعداد تقارير عن النتائج، وسيكون المدير وقتها هو المسؤول عن الرد على جميع الملاحظات الخاصة بالتدقيق وتنفيذ الإجراءات التصحيحية الموصى بها.

إن كبار المديرين بحاجة إلى فهم وإدراك مجمل عملية التدقيق الداخلي والكيفية التي يتم من خلالها جدولة وتنفيذ عمليات التدقيق الداخلي ومن ثم القيام بإعداد التقارير الخاصة بها. وبالرغم من احتمالية وجود العديد من الاختلافات، اعتماداً على حجم ودرجة تعقيد المنظمة وأهداف عملية التدقيق، فإن العملية النموذجية للتدقيق الداخلي تحتاج إلى جدولة عملية المراجعة والقيام بتقييم المخاطر وتنفيذ إجراءات التدقيق الضرورية، ومن ثم إعداد تقارير عن نتائج التدقيق وإرسالها إلى إدارة ولجنة التدقيق. لسنا هنا بصدد وصف الكيفية التي يتم من خلالها تنفيذ عمليات التدقيق الداخلي، ولكننا نهدف بشكل عام إلى تحقيق فهم لهذه العملية. ومع ذلك فالنقطة الأساسية هنا هي أن الأشخاص الذين يقومون بتنفيذ عمليات التدقيق الداخلي لا ينبغي أن يتصرفوا بصفة استشاريين داخليين. وكما وضحنا في وصفنا المختصر للمعايير المهنية للتدقيق الداخلي في القسم التالي، فإنه يتعين على المديرين التنفيذيين الذين لم يشاركوا بشكل مباشر في عملية التدقيق الداخلي أن يدركوا أن الدور الرئيسي للتدقيق الداخلي هو فحص ومراجعة واختبار الضوابط الداخلية والعمليات المرتبطة بها. أما إذا تصرفت وحدة التدقيق الداخلي كما لو كانت هيئة استشارية داخلية، وجب أن يتم اتخاذ ترتيبات منفصلة، وفي مثل هذه الحالة يتعين على جميع الأطراف أن تدرك أن الأنشطة الاستشارية الداخلية منفصلة ومختلفة عن أنشطة التدقيق الداخلي.

عملية التدقيق الداخلي: التخطيط لعمليات التدقيق الداخلي ومنح الترخيص الخاص بها:
إن إدارة التدقيق الداخلي في المؤسسة النموذجية ليست إدارة منفصلة، مثل إدارة المشتريات أو حساب المقبوضات أو الإدارة الهندسية، وإنما إدارة التدقيق الداخلي وكذلك رئيس التدقيق الداخلي - يسمى عادة مدير التدقيق الداخلي (CAE) - هو من يقوم بإعداد التقارير وإرسالها مباشرة إلى لجنة التدقيق التابعة لمجلس الإدارة. وقد تم فرض هذا المطلب في الولايات المتحدة، من قبل هيئة الأوراق المالية والبورصة الأمريكية (SEC). وعلى الرغم من أنه قد يكون لعملية التدقيق الداخلي علاقة اسمية بعملية إعداد التقارير وإرسالها إلى المدير المالي (CFO) أو بعض الوظائف الإدارية الأخرى، فإنه يجب أن يكون للتدقيق الداخلي علاقة مستقلة مع لجنة التدقيق.

ويتم التكليف للقيام بأنشطة التدقيق الداخلي من خلال وثيقة رسمية تعرف بميثاق التدقيق الداخلي، والتي تتم الموافقة عليها من قبل لجنة التدقيق، ويُمنح فريق التدقيق الداخلي السلطة الكاملة لإجراء مراجعات مستقلة وفحص للمواد. فمن منظور حوكمة تقنية المعلومات، على سبيل المثال، فإن وثيقة الميثاق تُعطي فريق التدقيق الداخلي السلطة للدخول على العمليات التشغيلية لمركز البيانات ومراجعة التقارير والمواد السرية الأخرى التي تعد جزءاً من عمليات التدقيق المخطط لها.

الشكل التوضيحي (١٩-١) يُعد مثالاً لميثاق التدقيق الداخلي لإحدى الشركات، وهي الشركة العالمية لمنتجات الحاسب (Global Computer Products)، وهو نموذج الشركة الذي تم استخدامه سابقاً. إذ يبين هذا الميثاق بوضوح "تعليمات التقدم marching orders" الخاصة بإحدى إدارات التدقيق الداخلي. وعندما يكون لدى المسؤول التنفيذي للشركة أي شكوك تتعلق بأنشطة وسلطة المدققين الداخليين، ينبغي عليه أن يطلب الاطلاع على نسخة من ميثاق التدقيق الداخلي الخاص بهم. فإذا تبين أن هذا الميثاق قد أهمل بعض المجالات كالقضايا المتعلقة بحوكمة تقنية المعلومات أو أنه منتهي الصلاحية، فإنه يتعين على المسؤول التنفيذي أن يطلب من رئيس لجنة التدقيق CAE الشروع في إجراءات تحديث الميثاق.

شكل توضيحي (١٩-١)

عينة لميثاق التدقيق الداخلي

إدارة التدقيق الداخلي
ميثاق تصريح
<p>مهمة التدقيق الداخلي:</p> <p>إن مهمة التدقيق الداخلي للشركة العالمية لمنتجات الحاسب (Global Computer Products) هو التأكد من أن عمليات الشركة تتبع معايير عالية، وذلك من خلال توفير إدارة ضمان مستقلة وموضوعية وتقديم المشورة بشأن أفضل الممارسات. فباستخدام نهج منظم ومنضبط، يساعد التدقيق الداخلي الشركة العالمية لمنتجات الحاسب على تحقيق أهدافها من خلال تقييم وتحسين فاعلية إدارة المخاطر والرقابة الداخلية وعمليات الحوكمة.</p>
<p>الاستقلالية والموضوعية:</p> <p>لضمان الاستقلالية فإن تقارير التدقيق الداخلي تُقدّم مباشرة إلى لجنة التدقيق التابعة لمجلس الإدارة، وللحفاظ على الموضوعية، فإن التدقيق الداخلي لا يشارك في عمليات التشغيل اليومية للشركة أو إجراءات الرقابة الداخلية.</p>
<p>النطاق والمسؤوليات:</p> <p>يشمل نطاق عمل التدقيق الداخلي مراجعة إجراءات إدارة المخاطر والرقابة الداخلية ونظم تقنية المعلومات وعمليات الحوكمة. ويشمل هذا العمل أيضاً الاختبار الدوري للمعاملات ومراجعة أفضل الممارسات والتحقيقات الخاصة وتقييم المتطلبات القانونية والتنظيمية والقياسات للمساعدة في منع واكتشاف الاحتيال.</p> <p>للوفاء بمسؤولياتها، يتعين على التدقيق الداخلي:</p> <ul style="list-style-type: none"> - تحديد وتقييم المخاطر المحتملة لعمليات تشغيل المؤسسة. - مراجعة مدى كفاية الضوابط الموضوعية لضمان الامتثال للسياسات والخطط والإجراءات وأهداف العمل. - تقييم موثوقية وأمن المعلومات المالية والإدارية والنظم الداعمة وعمليات التشغيل التي تُنتج هذه المعلومات. - تقييم وسائل حماية الأصول. - مراجعة العمليات القائمة واقتراح تحسينات لها. - تقييم استخدام الموارد فيما يتعلق بالاقتصاد والكفاءة والفاعلية. - متابعة التوصيات للتأكد من أن الإجراءات التصحيحية الفعالة يتم اتخاذها وتطبيقها فعلاً. - تنفيذ التقييمات أو التحقيقات أو المراجعات المتعلقة بموضوع ما والمطلوبة من قبل لجنة التدقيق والإدارة.

<p>سلطة التدقيق الداخلي:</p> <p>من أجل تعزيز ضوابط فعالة بتكلفة معقولة، يُصرَّح للتدقيق الداخلي، في حدود نطاق أنشطته، بأن يقوم بـ:</p> <ul style="list-style-type: none"> - دخول جميع مناطق عمليات التشغيل للشركة العالمية لمنتجات الحاسب والحصول على أي وثائق وسجلات تعتبر ضرورية لإتمام المهام المكلفة بها. - مطالبة جميع أعضاء طاقم العمل والإدارة بتزويدهم بالمعلومات والإيضاحات المطلوبة خلال فترة زمنية معقولة.
<p>المساءلة:</p> <p>يتعين على التدقيق الداخلي أن يقوم، بالتنسيق مع إدارة ولجنة التدقيق، بإعداد الخطة السنوية للتدقيق التي تعتمد على مخاطر العمل ونتائج التدقيقات الداخلية الأخرى، ومدخلات الإدارة. ويجب أن تُقدَّم الخطة للإدارة العليا، متضمناً ذلك المستشار العام، للموافقة عليها من قبل لجنة التدقيق. وإن كان هناك أي تعديلات ضرورية على الخطة ينبغي إرسالها للموافقة عليها من قبل لجنة التدقيق.</p> <p>إن التدقيق الداخلي هو المسؤول عن التخطيط والتوجيه وإعداد وتقديم التقارير ومتابعة مشاريع التدقيق المدرجة في خطة التدقيق واتخاذ قرار بشأن نطاق وتوقيت هذه التدقيقات. وسيتم الإبلاغ عن نتائج كل عملية من عمليات التدقيق الداخلي من خلال تقرير التدقيق التفصيلي الذي يلخص أهداف ونطاق التدقيق وكذلك الملاحظات والتوصيات. وفي جميع الحالات، سيضطلع عمل المتابعة بضمان الاستجابة الكافية لتوصيات التدقيق الداخلي. وسوف يُقدَّم التدقيق الداخلي أيضاً تقريراً سنوياً إلى الإدارة العليا وإلى لجنة التدقيق حول نتائج أعمال التدقيق، متضمناً ذلك التعرض للمخاطر المؤثرة وقضايا الرقابة.</p>
<p>المعايير:</p> <p>يلتزم التدقيق الداخلي للشركة العالمية لمنتجات الحاسب بالمعايير والممارسات المهنية الصادرة عن معهد المدققين الداخليين ومعهد حوكمة تقنية المعلومات كذلك.</p>

بينما قد تُلزم أو تطلب لجنة التدقيق من الرئيس التنفيذي للتدقيق الداخلي CAE وإدارة التدقيق الداخلي التابعين لها، القيام بإجراء إحدى المراجعات المحددة للتدقيق الداخلي؛ يقوم التدقيق الداخلي عادة من خلال التقييمات المستمرة للمخاطر أو طلبات الأعضاء الآخرين في الإدارة أو من خلال خبراتها المكتسبة من عمليات أخرى كانت قد أجرتها للتدقيق الداخلي - بتطوير خطط قصيرة الأجل وأخرى طويلة الأجل لعمليات التدقيق الداخلي التي تُخطط لتنفيذها خلال الفترة القادمة. فبالاعتماد على هذه الخطة وكذلك على عمليات التدقيق المكتملة في الماضي القريب، يتعين على الرئيس التنفيذي للتدقيق

CAE اتخاذ جميع التدابير والترتيبات الضرورية الخاصة بموظفي التدقيق الداخلي وغيرها من الموارد لتنفيذ هذا البرنامج الخاص بعمليات التدقيق الداخلي المخطط لها للمؤسسة.

عملية التدقيق الداخلي: تدشين عملية التدقيق الداخلي:

يوضح الشكل التوضيحي (١٩-٢) العمليات اللازمة لإجراء عملية التدقيق الداخلي المكونة من أربعة مراحل أو خطوات مختصرة. ومع أن الخطة السنوية تستلزم أن يتم إجراء التدقيق الداخلي في أحد المناطق، فإنه من باب المجاملة، وبشكل عام تقتضي أن يقوم التدقيق الداخلي بالعمل مع المنطقة التي يتم مراجعتها لجمع بعض التفاصيل الأولية حول المنطقة محل المراجعة وجدولة عملية التدقيق. هناك العديد من النشاطات لكل مرحلة من المراحل الموضحة بالشكل. على سبيل المثال، تدعو المرحلة ذات المستوى الأعلى إلى:

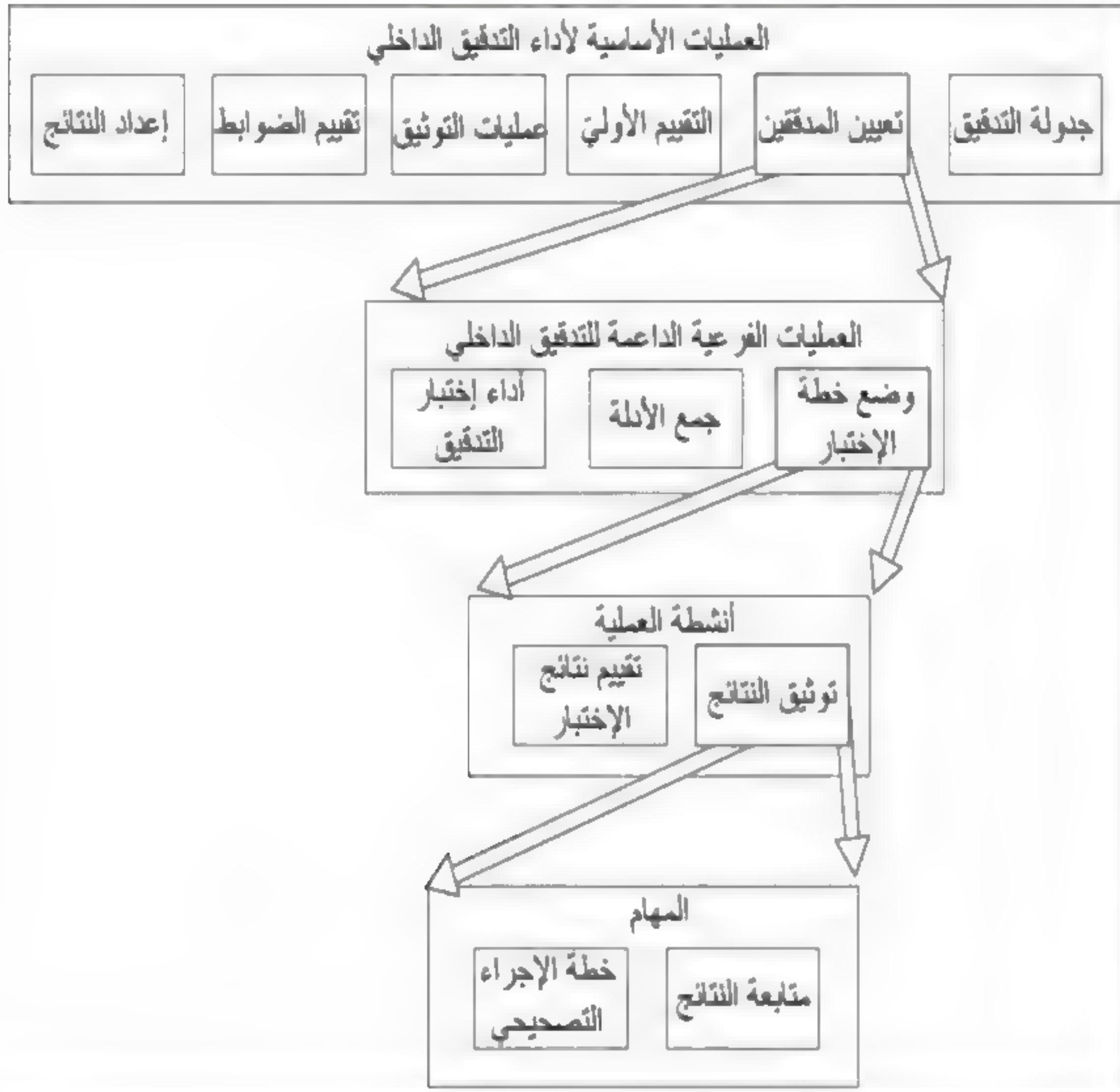
- **جدولة التدقيق:** بعد أن تم وضع الخطة السنوية الشاملة للتدقيق والمعتمدة من قبل لجنة التدقيق، يجب أن يتم وضع جدول زمني لعملية التدقيق المحددة، مع الأخذ بعين الاعتبار الاحتياجات الخاصة بموارد التدقيق واعتبارات الوقت الخاصة بالجهة الخاضعة للتدقيق، وغيرها من العوامل.

- **تعيين المدققين:** يكون هناك غالباً ندرة في الموارد البشرية العاملة في تدقيق تقنية المعلومات. لذا يجب إيلاء المزيد من الحرص والاهتمام لعملية تعيين أخصائيي تدقيق تقنية المعلومات للمهام المناسبة، في حين أن المدققين الداخليين ذوي المهارات الأخرى ينبغي أن يتم تعيينهم في الأماكن الأنسب لهم.

- **إجراء التقييمات الأولية للتدقيق:** قد يقوم التدقيق الداخلي بجدولة عمليات المراجعة الخاصة بتقييم الضوابط الداخلية لإحدى النظم أو العمليات، ولكن قبل البدء في العمليات الفعلية للتدقيق، يكون من الضروري القيام بجمع المزيد من المعلومات المتعلقة بالمنطقة المراد مراجعة عملياتها وإجراء بعض التقديرات الأولية حول مداها وعمقها وجميع الضوابط الداخلية والمخاطر المرتبطة بها، وبالأساليب المستخدمة لتقييم المنطقة المراد مراجعتها.

شكل توضيحي (٢-١٩)

عملية أداء التدقيق الداخلي



- توثيق العمليات الخاصة بالمنطقة التي يتم تدقيقها: يعد التوثيق المناسب مطلباً رئيسياً لجميع أعمال التدقيق الداخلي. ولا يكفي القول بأن لدى إحدى العمليات ضوابط داخلية كافية. فالمدقق الداخلي يجب عليه أن يقوم بجمع الأدلة الوثائقية لإثبات أن هذه الضوابط كافية في الوقت الذي يقوم فيه المدقق بالمراجعة.

• **تقييم الضوابط الداخلية:** إن تقييم الضوابط الداخلية في الحقيقة هو جوهر عملية التدقيق الداخلي. فالمدقق الداخلي يأخذ الضابط الداخلي الذي هو بصدد تقييمه ويقوم بوضع خطة اختبار لتقييم هذا الضابط. وقد يحتاج ذلك إلى جمع أدلة التدقيق وإجراء اختبارات التدقيق، كما هو مبين في المستوى التالي للعمليات الموضحة بالشكل.

• **تحضير وإعداد النتائج:** يقوم المدقق الداخلي باختبار وتقييم الضوابط الداخلية من خلال استخدام مجموعة متنوعة من الأساليب، والتي تبدأ من الاختبار الرسمي للمعاملات إلى الحصول على الانطباعات من خلال المقابلات أو الملاحظات، وهي تسمى غالباً نتائج التدقيق الداخلي. وقد تجد نتائج وملاحظات الاختبار هذه طريقها أخيراً إلى تقرير رسمي للتدقيق الداخلي يلخص تلك النتائج والتوصيات الخاصة بالتدقيق.

لقد قمنا للتو بوصف الخطوات الرئيسية في عملية التدقيق الداخلي، فالمدقق الداخلي سوف يمر بالنمط نفسه من الخطوات في كل منطقة من المناطق التي يقوم بمراجعتها. لا يهدف هذا الفصل إلى تقديم وصف شامل للكيفية التي يتم من خلالها إجراء عملية التدقيق الداخلي لكبار المسؤولين التنفيذيين، ولكن يهدف إلى إعطاء فهم للعمليات اللازمة لإجراء التدقيق الداخلي المناسب. ستبقى هذه الخطوات الأساسية هي نفسها سواء أكانت لمراجعة الضوابط المالية لإحدى العمليات أم لمراجعة أحد تطبيقات النظم الخاصة بتقنية المعلومات.

عملية التدقيق الداخلي: مراجعة أدلة التدقيق واختبارها:

يحتاج الجزء الأكبر من عملية التدقيق الداخلي إلى جمع ومراجعة واختبار ما يُطلق عليه المدققون الداخليون اسم أدلة التدقيق Audit evidence. فقد يسأل المدقق الداخلي عن حالة التوثيق الخاصة بأحد التطبيقات الجديدة لتقنية المعلومات، ويتم إخباره بأن التوثيق "حديث". فإذا كان النظام أو التطبيق ثانوياً، فقد يقوم المدقق باعتماد وتدوين تلك الإجابة والمضي قدماً. في جميع الأحوال فلكي يكون لدينا أدلة قوية على حداثة ذلك التوثيق، فقد يقوم المدقق الداخلي بطلب مراجعة التوثيق الفعلي للتأكد من وجودها. ولمزيد من التفاصيل، قد يقوم المدقق الداخلي بالتعمق أكثر في التوثيق وفحص أمور منها على سبيل المثال مدى ملاءمة التنقيحات التي تمت عليها، أو أن يقوم بإجراء المزيد من الفحوصات المختلفة ليرى ما إذا كانت هذه الوثيقة كافية وداعمة لضوابط النظام.

تتطلب هذه العملية برمتها أن يقوم المدقق الداخلي بتقييم مدى كفاية أدلة التدقيق الموجودة وإجراء بعض التقييمات بناء على عمل التدقيق الداخلي. الشكل التوضيحي (٣-١٩) يبين أنواعاً مختلفة من أدلة التدقيق من الأقوى إلى الأضعف. ويبين العمود الأول أنواع أدلة التدقيق، فتقنية التدقيق الخاصة بمشاهدة ممارسة ما على أرض الواقع تعد أقوى بكثير من مجرد الإخبار عن تلك الممارسة. لا توجد أي مطالبة تتعلق بوجوب دعم كل أعمال التدقيق الداخلي من قبل أقوى مستويات الأدلة. حيث إن طبيعة التدقيق الداخلي والمخاطر المرتبطة بها تعد من العوامل المحددة للمستوى المطلوب لأدلة التدقيق، فإنه يجب دائماً على المدير الأول الذي يعمل مع المدققين الداخليين ويقوم بمعالجة التوصيات الناتجة عنهم أن يأخذ في الحسبان الطريقة التي يستخدمها هؤلاء المدققون في جمع أدلة التدقيقات الداعمة لنتائجهم واستنتاجاتهم الموثقة.

عملية التدقيق الداخلي: تقديم التقارير الخاصة بنتائج التدقيق الداخلي:

يجب أن تُختتم الأعمال الخاصة بعملية التدقيق الداخلي بتقرير رسمي يصف الأهداف التي من أجلها تمت هذه المراجعة في منطقة ما، وما الإجراءات المتبعة لتقييم الضوابط الداخلية الخاصة بهذه الأهداف التدقيقية، وما الذي تم اكتشافه، وما إذا كانت الضوابط الداخلية الموجودة قد قُيِّمت بشكل كافٍ أم لا. في معظم الحالات، نجد أن هذه التقارير الخاصة بعملية التدقيق سوف تؤدي إلى توصيات رسمية تتعلق بإجراء تحسينات على الرقابة الداخلية بناء على نتائج التدقيق في المجال الذي تمت مراجعته. وعلى الرغم من أن الممارسات قد تختلف باختلاف المؤسسات، فإن تقارير التدقيق الداخلي عموماً ستحتاج إلى استجابة إدارية رسمية تُقر بنتائج التدقيق الداخلي وتوضح الكيفية التي سيستخدمونها لتصحيح أوجه القصور في الرقابة المبلغ عنها بالتقرير.

شكل توضيحي (٣-١٩)

تصنيفات جوانب قوة التدقيق الداخلي الخاصة بأدلة التدقيق

تصنيفات أدلة التدقيق الداخلي التي تم جمعها	الأدلة الداعمة القوية لاستنتاجات التدقيق	أضعف المستويات لأدلة التدقيق الداخلي
أسلوب التدقيق	الملاحظات / التأكيدات	استفسار
أصل الأدلة	مدعوم	إحصائيات أساسية
العلاقة مع الجهة الخاضعة للتدقيق	إدارة خارجية	مجموعة داخلية
شكل الأدلة	مكتوب / نظام مؤمن	شفهي
تطور الأدلة	رسمي / موثق	غير رسمي
موقع الأدلة	تم إنشاؤه في نظام فعلي	مستمدة من نظام الدعم
مصدر أدلة التدقيق	عمل تدقيق شخصي	مُورَد "مستعمل"

لا يتم تعميم التقارير الخاصة بعملية التدقيق على المؤسسة. فهي تكون عادة موجهة فقط إلى منطقة محددة من مناطق المؤسسة التي تمت مراجعة عملياتها وإلى مديريها المباشرين وإلى الإدارة العليا في المؤسسة كذلك، مثل الرئيس التنفيذي والمدير المالي وشريك التدقيق الخارجي ولجنة التدقيق. إن نتائج التدقيق السيئة لعمليات التشغيل في إحدى الوحدات التي تمت مراجعتها سوف تؤدي إلى جعل التركيز بالفعل ينصب على الإدارة للقيام بتصحيح أو إصلاح أوجه القصور في الرقابة الداخلية في تلك الوحدة. وقد يكون ذلك أحد العناصر الهامة في حوكمة تقنية المعلومات.

يواجه المدققون الداخليون غالباً في العديد من المناطق التي يقومون فيها بمراجعة عملياتها مشاكل تتعلق بضيق الوقت وقلة الموارد اللازمة لمراجعة وتدقيق جميع المناطق ذات المخاطر العالية في المؤسسات الكبيرة بصورة كافية. فعلى سبيل المثال، كان مؤلف هذا الكتاب في فترة من الفترات يعمل مديراً لإحدى عمليات التدقيق الداخلي الخاصة بإحدى الشركات الأمريكية الكبرى التي تحتوي على العديد من الوحدات التشغيلية، وكان لكل وحدة تشغيلية ثلاثة من مديري التدقيق الداخلي وما يقارب ثمانين موظفاً يعملون في مجال التدقيق الداخلي. فعلى الرغم من التحليل المكثف للمخاطر والخطط السنوية

المنظمة جيداً لعمليات التدقيق الداخلي، فإنه كان من الصعب استكمال جميع عمليات التدقيق المخطط لها وتغطية جميع المخاطر. لذا تم تعديل الخطط وإعادة ملاءمتها بصورة منتظمة بسبب الأزمات الجديدة للأعمال التي تتطلب المزيد من أنشطة التدقيق. إن الأنشطة الاحتياطية المكتشفة حديثاً، على سبيل المثال، من شأنها أن تحول أنشطة التدقيق الداخلي الأخرى للمساعدة في التحقيق في مزاعم الاحتيال على نحو أفضل.

وينبغي على القارئ الذي يريد الحصول على مزيد من المعلومات حول التدقيق الداخلي ودوره في حوكمة تقنية المعلومات أن يعود إلى كتاب المؤلف السالف الذكر، التدقيق الداخلي الحديث لبرينك (Brink's Modern Internal Auditing). فهذا الكتاب يضع تعريفاً لهيكل المعرفة الشائع للتدقيق الداخلي، والمجالات الواسعة التي يجب على المدقق الداخلي أن يعرفها ويفهمها.

معايير التدقيق الداخلي الخاصة بحوكمة تقنية المعلومات:

إن المنظمة المهنية للمدققين الداخليين، معهد المدققين الداخليين (IIA)، هي المسؤولة عن إصدار معايير الممارسة والسلوك لجميع المدققين الداخليين، وذلك على أساس عالمي. هذه الإرشادات الرسمية عبارة عن مزيج من بيانات المعايير الإلزامية المطلوبة والضرورية لممارسة مهنية مستمرة لعملية التدقيق، بالإضافة إلى سلسلة من ممارسات المعايير الموصى بها بقوة. إن هذه المعايير الخاصة بمعهد المدققين الداخليين تذهب إلى ما هو أبعد من أن تكون مجرد معايير لحوكمة تقنية المعلومات، فهي تغطي نشاطات التدقيق الداخلي للحوكمة على أساس واسع. فعلى سبيل المثال، ينص المعيار 2110. A2 لمعهد المدققين الداخليين IIA والخاص بالأداء على أن:

"نشاط التدقيق الداخلي يجب أن يُقيّم ويحدد ما إذا كانت حوكمة تقنية المعلومات التابعة للمنظمة تحافظ على إستراتيجيات وأهداف المنظمة وتدعمها."

وعلى الرغم من الأسلوب العام المستخدم في صياغة المعيار، فإنه يطلب في الأساس من المدقق الداخلي أن يقوم بتقييم ما إذا كانت البنية التحتية لتقنية المعلومات في المؤسسة ملائمة وكافية للعمليات التشغيلية للأعمال والمحافظة عليها بحيث يتم إدارة جميع الأهداف الطويلة الأجل للمؤسسة بأكملها بشكل صحيح.

إجراءات التدقيق الداخلي الخاصة بحوكمة تقنية المعلومات:

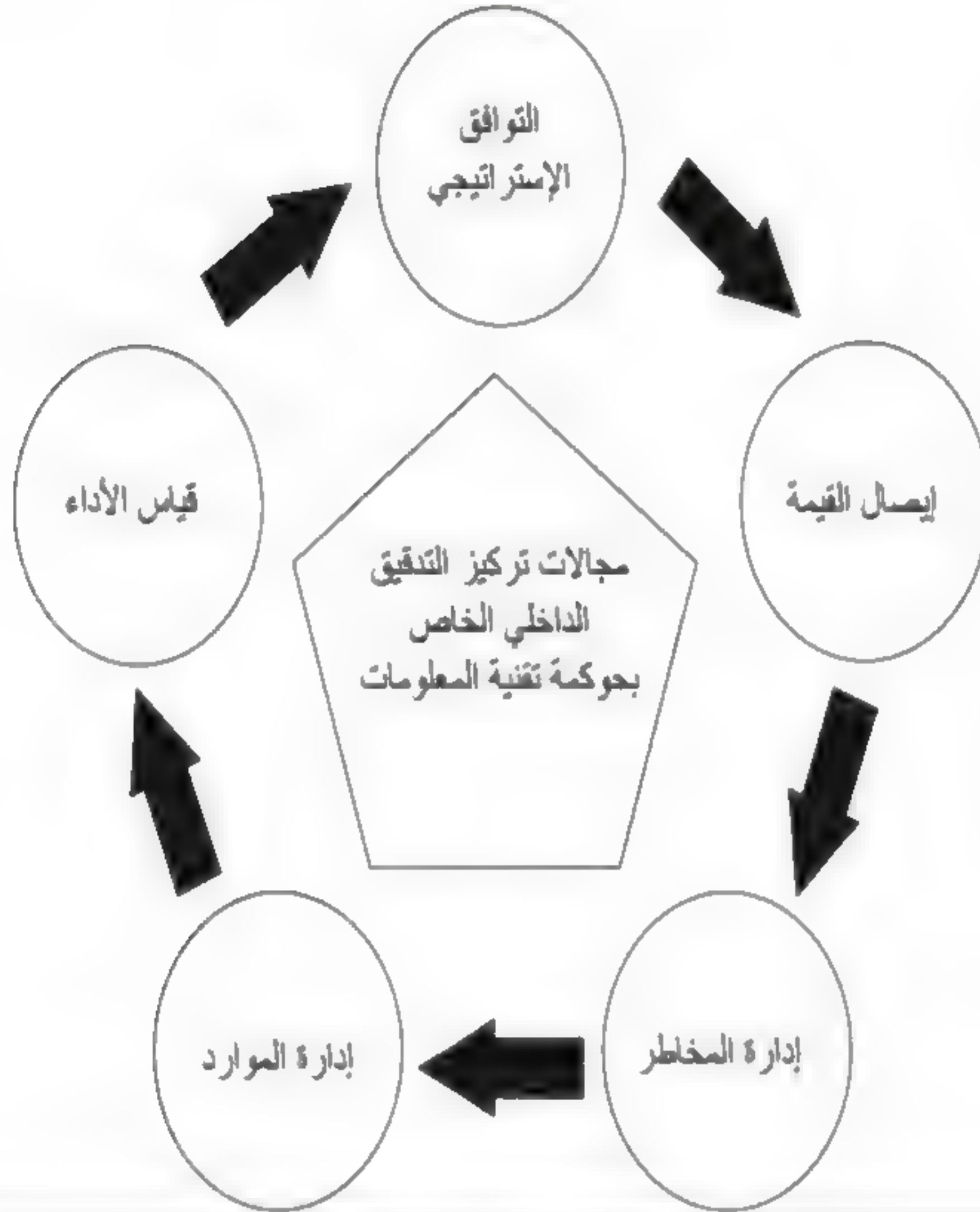
استناداً إلى حديثنا في الفصول السابقة عن حوكمة تقنية المعلومات، فإن الأهداف الرئيسية لحوكمة تقنية المعلومات هي التأكد من أن الاستثمارات في تقنية المعلومات تُوجد قيمة للأعمال، وتخفف من المخاطر المرتبطة بعمليات ونظم تقنية المعلومات. يمكن للعديد من الأنشطة الخاصة بمراجعات عمليات التدقيق الداخلي أن تلعب دوراً رئيسياً في دعم حوكمة تقنية المعلومات في المؤسسة. مثال على ذلك، نشاط التدقيق الداخلي المستمر لتقنية المعلومات عبارة عن مراجعات وتقييمات للخطط الخاصة باستمرارية تقنية المعلومات المؤسسية، التي كانت تسمى في فترة من الفترات خطط التعافي من كوارث تقنية المعلومات في زمن نظم الحاسبات المركزية. وإن إدارة تقنية المعلومات في المؤسسة تحتاج إلى عمليات معمول بها لاستعادة العمليات التشغيلية والموارد الخاصة بتقنية المعلومات وإعادة تأهيلها إلى مستوياتها التشغيلية الطبيعية في حال حدوث عطل ما طويل الأجل في خدمات تقنية المعلومات. إن مراجعات وتقييمات التدقيق الداخلي في هذا المجال تدعم إلى حد كبير عمليات حوكمة تقنية المعلومات في المؤسسة.

وقد تدعم عمليات التدقيق الداخلي إلى حد كبير العمليات الخاصة بحوكمة تقنية المعلومات المؤسسية من خلال إجراء المراجعات والتقييمات في هذه المجالات العامة. الشكل التوضيحي (١٩-٤) يحدد خمسة مجالات عامة يجب أن يركز عليها التدقيق الداخلي أثناء مراجعاته لحوكمة تقنية المعلومات: إيصال القيمة وإدارة المخاطر والموارد والأداء وقضايا التوافق الإستراتيجي. إن المعايير المهنية للتدقيق الداخلي تتطلب المستويات التالية من أنشطة أعمال المراجعة لعملية التدقيق الداخلي:

- مراجعة وتقييم عملية إيصال القيمة المرجوة من إدارة تقنية المعلومات، وكيف تتماشى تقنية المعلومات مع رسالة ورؤية وقيم وأهداف وإستراتيجيات المنظمة.
- مراجعة ما إذا كان لدى إدارة تقنية المعلومات بيان واضح عن الأداء المتوقع للعمل (من حيث الفاعلية والكفاءة) وتقييم مدى إنجازه.
- مراجعة وتقييم فاعلية عمليات إدارة موارد تقنية المعلومات وأدائها.

شكل توضيحي (٤-١٩)

مجالات تركيز التدقيق الداخلي لحوكمة تقنية المعلومات



- مراجعة وتقييم التوافق مع المتطلبات القانونية والبيئية ومتطلبات جودة المعلومات والمتطلبات الائتمانية والأمنية.
- مراجعة وتقييم البيئة الرقابية للمنظمة.
- مراجعة وتقييم المخاطر التي قد تؤثر سلباً في بيئة تقنية المعلومات.

يجب أن يدرك ويعترف المدبرون التنفيذيون للأعمال غير المشاركون في مهام التدقيق الداخلي بأن إدارة التدقيق الداخلي هي كيان مستقل في المؤسسة، ولا يستطيع أي مدير تنفيذي من خارج لجنة التدقيق أن يقوم بإعطاء توجيهات لعملية التدقيق الداخلي للقيام بإجراء مراجعات في منطقة ما. وأن خطط مراجعة التدقيق الداخلي الخاصة بهم ينبغي ألا يتم وضعها إلا من خلال موافقة لجنة التدقيق. ومع ذلك، ينبغي أن يشعر الموظفون التنفيذيون للعمليات التشغيلية في المؤسسة أو إدارة تقنية المعلومات بأن لديهم مطلق الحرية في أن يسألوا الرئيس التنفيذي للتدقيق وغيره من أعضاء إدارة التدقيق الداخلي عن خططهم وأنشطتهم الحالية في مراجعة النواحي الرئيسية التي تخص حوكمة تقنية المعلومات في المؤسسة.

مراجعات التدقيق الداخلي لعمليات التوافق الإستراتيجي لتقنية المعلومات:

ومن ضمن الخطط السنوية والأنشطة الجارية لإدارة تقنية المعلومات في المؤسسة، أنه يجب على التدقيق الداخلي القيام بتقييم ما إذا كانت تلك الخطط والعمليات التشغيلية الخاصة بتقنية المعلومات تنسجم مع أنشطة الأعمال الأخرى في المؤسسة. العنصر الرئيسي لتحقيق ذلك هو أنه يجب على جميع العمليات التشغيلية لتقنية المعلومات، متضمناً ذلك تطوير النظم وإدارة الجودة ومعالجة تقنية المعلومات أن تنسجم مع العمليات التشغيلية للأعمال. بمعنى أنه يجب أن يكون للعمليات التشغيلية لتقنية المعلومات قيمة وموقع تنافسي في المنتجات والخدمات التي تقدمها المؤسسة. إن إدارة تقنية المعلومات يجب أن تسعى جاهدة للحفاظ على تكاليفها من خلال تحسين الكفاءة والفاعلية الإدارية. وعلى الرغم من أن هذه الأمور تمثل كل النداءات الخاصة بإدارة تقنية المعلومات والإدارة العامة، فإنه يجب دائماً على إدارة التدقيق الداخلي القيام بطرح بعض الأسئلة الصعبة أثناء قيامها بمراجعة أنشطة الأعمال.

كما ذكرنا سابقاً، فإن الإدارة الفعالة لتقنية المعلومات ينبغي أن يكون لديها نوع من أنواع اللجان التوجيهية، التي تقوم بمهمة التخطيط الطويل الأجل حيث يمكن أن يلتقي مزيج متنوع من مستخدمي موارد تقنية المعلومات مع إدارة تقنية المعلومات ليقوموا بمراجعة أو الموافقة على المقترحات الجديدة وتحديد الأولويات المتعلقة بالأعمال الجديدة.

يجب على عمليات تدقيق تقنية المعلومات أن توصي وتشدد على وجود وجاهزية هذه الإدارة الفعالة، كما يجب أن تشارك في أغلب الاجتماعات التي تجريها تلك اللجنة التوجيهية. ويجب أن تقوم اللجنة التوجيهية بوضع إستراتيجية بعيدة المدى لأنشطة واستثمارات تقنية المعلومات والمراجعات الدورية للتدقيق الداخلي، من خلال المشاركة غير الفعالة في جلسات اللجنة التوجيهية أو المراجعات الرسمية للتدقيق الداخلي، وينبغي تأكيد أن تكون هذه الإستراتيجية لتقنية المعلومات في موضوع التنفيذ وجاهزة للعمل.

لا بد من وجود نهج متكامل لعمل المؤسسة وإستراتيجية تقنية المعلومات، ومهام ذات مسؤولية تشاركية بينهما. وبالإضافة إلى ذلك، وعلى الرغم من أن إدارات تقنية المعلومات تكون ملامة أحياناً على تبنيها لأساليب جديدة وغير مجربة، فإنه يجب أن يكون هناك تصريح واضح بأهداف تلك الأساليب المتبعة. وقد تمثل عملية التدقيق الداخلي من خلال مراجعاتها وتعليقاتها التدقيقية الصوت الفعال للمساعدة في ضمان تحقيق هذه الأهداف.

مراجعات التدقيق الداخلي لعمليات إيصال قيمة تقنية المعلومات:

يجب أن تكون مراجعات التدقيق الداخلي مصممة لضمان استمرار تقديم تقنية المعلومات لفوائدها المرجوة وفق إستراتيجياتها المعلنة. إن الفكرة هنا هي أن المشاريع الجديدة لتقنية المعلومات، سواء كانت عمليات تطبيقية جديدة أو محسنة أم أدوات ومعدات جديدة يتم اقتراحها للحصول على الفوائد المتوقعة. ومع أنه من المؤكد أن عملية التدقيق الداخلي لن تكون قادرة على مراجعة جميع هذه الأعمال، نتيجة الأولويات المفروضة ومحدودية الموارد، فإنه يجب القيام بعملية تقييم دوري للفوائد المعلنة لاكتشاف ما إذا كانت الأهداف المعلنة قد تم تحقيقها بالفعل أم لا. ينبغي أن يبحث التدقيق الداخلي عن عوائد الاستثمار الرسمية، والتكلفة الإجمالية للملكية، ووسائل لقياس أعمال تقنية المعلومات.

وكما تحدثنا في الفصل السادس عشر من هذا الكتاب عن موضوع إدارة المشروعات، فإن إدارة تقنية المعلومات المؤسسية ينبغي أن يكون لديها عملية رسمية متعارف عليها ومعمول بها لإدارة مشاريع تقنية المعلومات لإيصال الفوائد إلى العمليات التشغيلية للأعمال. إن تقييم إيصال القيمة يتجاوز كثيراً العمليات التقليدية للتدقيق الداخلي التي تركز على

الضوابط الداخلية، ويتطلع لإيصال قيمة أفضل للعمليات التشغيلية لتقنية المعلومات. كما أن هناك حاجة إلى التزام رسمي لوضع منهجيات رسمية للتطوير الشامل لعملية تقديم خدمات تقنية المعلومات.

إن هذا المفهوم لمراجعات التدقيق الداخلي الخاصة بعمليات تقديم خدمات تقنية المعلومات يتجاوز الكثير من الجهود المبذولة في المراجعات الاعتيادية للتدقيق الداخلي. وقد ناقش الفصل السادس من هذا الكتاب موضوع تقديم خدمات تقنية المعلومات على أنه جزء من المفاهيم الخاصة بالإطار آيتل وإدارة خدمات تقنية المعلومات. إن الإدارة الفعالة للتدقيق الداخلي تحتاج لاستيعاب هذه المفاهيم ومزجها مع الإجراءات الأخرى للتدقيق الداخلي.

مراجعات التدقيق الداخلي لعمليات إدارة مخاطر تقنية المعلومات:

كما أكدنا في الفصل الثامن من هذا الكتاب الذي يدور حول إدارة المخاطر وفي الشروحات الأخرى طوال هذه الفصول؛ فإن إدارة المخاطر تعد مفهوماً مهماً جداً بالنسبة لحوكمة تقنية المعلومات، وأن فهمها ووضعها محل التقدير ينبغي أن يكون بالفعل جزءاً من جميع مراجعات التدقيق الداخلي. وهذا يتطلب توعية من كبار المسؤولين عن الرغبة في المخاطر الخاصة بالمؤسسة. لذا يجب تضمين مسؤوليات إدارة مخاطر تقنية المعلومات في جميع مستويات العمليات التشغيلية للأعمال. وهذا المجال يهتم غالباً بعمليات تقنية المعلومات حيث كانت هناك ميول تاريخية لتجربة أساليب جديدة للنظم أو التقنيات مع القليل من الفهم لأي مخاطر مرتبطة بها. وعلى الرغم من أن إدارة تقنية المعلومات ومستخدمي تقنية المعلومات ينبغي أن يكونوا هم المسؤولين في هذه الحالة، فإنه يكون هناك غالباً ميل لتجربة بعض الأساليب الجديدة وغير المجربة مع قليل من التفكير في المخاطر إذا فشلت. ويمكن للتدقيق الداخلي في كثير من الأحيان أن يكون فعالاً جداً من خلال أخذ دور محامي الشيطان في طرح الأسئلة الصعبة بوصفها جزءاً من مراجعاتها.

إن العمليات المناسبة لإدارة المخاطر ينبغي أن تركز على حماية أصول تقنية المعلومات ودعم النظم من خلال إجراءات التعافي من الكوارث والخطط الفعالة لاستمرارية العمليات التشغيلية. لقد كان هذا هو المجال التقليدي لمراجعات التدقيق الداخلي وتدقيق تقنية المعلومات، وينبغي تأكيدها على أنها جزء من أنشطة مراجعة حوكمة تقنية المعلومات.

ينبغي أن تركز جميع مراجعات التدقيق الداخلي على التوعية بمخاطر تقنية المعلومات على أساس من الشفافية لجميع أصحاب المصالح، ولا بد من بذل الجهود من أجل تضمين إدارة المخاطر باعتبارها جزءاً متكاملاً لامتحان وضمان المؤسسة. وينص ذلك حقيقة على أن إدارة التدقيق الداخلي يجب أن تذهب إلى ما هو أبعد من مجرد المراجعات المتخصصة لتدقيق تقنية المعلومات وإضافة مخاوف إدارة مخاطر تقنية المعلومات لجميع المراجعات التي تغطي مجالات حوكمة تقنية المعلومات. وبالإضافة إلى العمليات الشاملة للتدقيق الداخلي، فإن هناك حاجة إلى إنشاء تقييمات فعالة لإدارة العملية على أنها جزء من مراجعات التدقيق الداخلي.

مراجعات التدقيق الداخلي لعمليات إدارة موارد تقنية المعلومات:

يتعين على التدقيق الداخلي لتقنية المعلومات أن يراجع ويقيم بانتظام فاعلية عملياته الخاصة بإدارة موارد تقنية المعلومات وأدائها. ففي العديد من المؤسسات، تعد مرافق تقنية المعلومات وعملياتها التشغيلية إحدى الاحتياجات الرئيسية فيها - إن لم تكن الرئيسية - لموارد المؤسسة. وينبغي على الإدارة أن تستثمر في هذه الموارد الخاصة بتقنية المعلومات من خلال خطط رسمية لمشروعات طويلة المدى والعمليات المتبعة في وضع الميزانيات. وقد قامت الفصول الأخرى بتغطية مسائل تتعلق بإدارة موارد تقنية المعلومات من منظور عمليات التشغيل الشاملة. على سبيل المثال، الفصل الرابع عشر من هذا الكتاب ناقش أهمية إدارة محافظ وتهيئة تقنية المعلومات لتكون وسيلة لإدارة وضبط الأصول المتنوعة لتقنية المعلومات بشكل أفضل. وكذلك ناقش الفصل السابع عشر من هذا الكتاب اتفاقيات مستوى الخدمة ليكون وسيلة لتعزيز قيمة استثمارات الأعمال.

يجب على التدقيق الداخلي أن يخطط ويطور سلسلة من المراجعات في هذه المجالات الخاصة بإدارة موارد تقنية المعلومات. وفحوى ذلك أنه من الصعب على إدارة التدقيق الداخلي مجرد إطلاق مراجعة لإدارة موارد تقنية المعلومات، عندما يكون الموضوع والمجال تقريباً واسعاً جداً لمراجعة واحدة للتدقيق الداخلي. بل يجب على التدقيق الداخلي أن يطور وينفذ مراجعات متخصصة في العديد إن لم يكن جميع مجالات حوكمة تقنية المعلومات التي تمت مناقشتها في هذه الفصول.

مراجعات التدقيق الداخلي لعمليات قياس أداء تقنية المعلومات:

يجب تطوير تقنيات لقياس الأداء للمساعدة في ترجمة الإستراتيجيات إلى أفعال من أجل تحقيق وقياس إنجازات أهداف تقنية المعلومات. هذا النوع من الأدوات يمكن أن يقيس العلاقات والأصول اللازمة لتحقيق التركيز على العميل وكفاءات العملية والتسهيلات لمساعدة المؤسسة وإدارات تقنية المعلومات الخاصة بها بشكل كلي في التعلم والنمو. هذه الأنواع من الأدوات تتبع عملية تقديم المشاريع ومتابعة خدمات تقنية المعلومات.

الشكل التوضيحي (١٩-٥) يوضح أنواع أنشطة مراجعة وتقييم التدقيق الداخلي اللازمة لتعزيز حوكمة تقنية المعلومات في المؤسسة. إن هذا الشكل على مستوى عال جداً ولكن يؤكد أن المدققين الداخليين بحاجة إلى مراجعة نظم وعمليات تشغيل تقنية المعلومات للمساعدة في تحسين العمليات الشاملة للرقابة الداخلية للمؤسسة وتبسيط وتحسين هذه العمليات ورفع توصية بمجالات معينة لأتمتتها بشكل أفضل، واقتراح مجالات يتم عمل توحيد قياسي لعملياتها ونظمها بشكل أفضل.

إن مجالات مراجعة التدقيق الداخلي هذه تغطي مجموعة واسعة من أنشطة التدقيق التي تتجاوز شروحات التدقيق الداخلي السابق تلخيصها في هذا الفصل والتي تعد جزءاً من أفضل ممارسات التدقيق الداخلي الشائعة لاحتياجات المعرفة. إن الإدارة الفعالة للتدقيق الداخلي ينبغي أن تكون عنصراً رئيسياً في تعزيز العمليات الفعالة لحوكمة تقنية المعلومات في أي مؤسسة.

شكل توضيحي (١٩-٥)

أنشطة مراجعة التدقيق الداخلي لحوكمة تقنية المعلومات



ملاحظة:

١. الآن في طبعته السابعة، Brink's Modern Internal Auditing تم نشره من خلال جون وايلي واولاده، عن طريق روبرت ر. مولر كمؤلف.

الجزء السادس
حوكمة تقنية المعلومات وأهداف المؤسسة

الفصل العشرون

بناء ثقافة أخلاقية في محل العمل والحفاظ عليها

كما تحدثنا في الفصول السابقة، فإنه لا بد من دمج عمليات حوكمة تقنية المعلومات مع عمليات التشغيل الأساسية لأعمال المؤسسة ويجب أيضاً أن تقع مسؤولية ضمان العمليات الصحيحة لحوكمة تقنية المعلومات على عاتق إدارة كل وحدة تابعة أو وحدة أعمال في المؤسسة أينما كانت. وباعتبار المؤسسة أحد العناصر الأساسية في هذا الصدد، فإنه يجب عليها أن تلتزم بتحقيق أعلى معايير الأخلاق والنزاهة في جميع مجالات عملياتها التشغيلية. يجب أن تبدأ نزاهة المؤسسة بالتزام كل أصحاب المصلحة وكل موظف بالقيم الأساسية للمؤسسة وبمسؤوليته لأداء دوره بالشكل الذي يتوافق مع تلك القيم ويخدمها.

يناقش هذا الفصل أهمية أخلاقيات العمل، وسياسات الحوكمة في المؤسسة، وهياكل الإشراف والعمليات، والخطوات اللازمة لإنشاء إدارة فعالة لأخلاقيات العمل، ووضع وتطبيق قوانين فعالة للسلوك، وإنشاء لجنة فعالة لامتثال المؤسسة تحت رئاسة مجلس الإدارة. إن هدفنا هو ذكر بعض أفضل الممارسات التي يمكن للمؤسسة اتباعها وتطبيقها لإرساء ثقافة أخلاقية في مكان العمل.

لا تقتصر القضايا وأفضل الممارسات المذكورة في هذا الفصل على عمليات تشغيل تقنية المعلومات وحوكمة تقنية المعلومات بل تمتد لتشمل جميع جوانب المؤسسة. ومع ذلك، فإن أفضل الممارسات مثل مدونة قواعد السلوك الفعالة للمؤسسة وبيان المهمة (الرسالة) المدعومة من الإدارة العليا ينبغي أن تحصل على الدعم من جميع أصحاب المصلحة في المؤسسة. ويجب أن تكون النتيجة النهائية هي بناء الثقافة الأخلاقية في مكان العمل.

أهمية بيانات المهمة (الرسالة):

لقد ناقشت الفصول السابقة من هذا الكتاب العديد من القضايا الهامة في حوكمة تقنية المعلومات، وركز معظمها على الحاجة إلى وضع معايير وعمليات فعالة لحوكمة تقنية المعلومات، مثل الفصل السابع من هذا الكتاب المتعلق بمعايير الأيزو الخاصة بالحوكمة،

أو الفصل الثاني عشر من هذا الكتاب أيضاً الخاص ببيان خدمات عمليات تشغيل تقنية المعلومات. إذ يركز كل فصل من هذه الفصول على مجالات محددة لتحسين عمليات تشغيل تقنية المعلومات في المؤسسة. في جميع الأحوال، فإن البيان الفعال لمهمة أو رسالة المؤسسة، والذي يغطي كل جوانب عمليات التشغيل وجميع أصحاب المصلحة، ينبغي أن يكون عنصراً أساسياً في إرساء ممارسات فعالة لحوكمة تقنية المعلومات.

تحتاج كل مؤسسة بغض النظر عن حجمها إلى بيان مهمة أو رسالة لوصف جميع أهدافها وقيمها. وينبغي أن تكون تلك الرسالة بمثابة مصدر للتوجيه - بوصلة - تسمح للموظفين والعملاء والمساهمين وغيرهم من أصحاب المصلحة بمعرفة ما تمثله المؤسسة وما لا تمثله. لقد كان بيان الرسالة في السنوات الماضية في كثير من الأحيان أكثر بقليل من مجرد شعار لطيف لكنه يبدو مُرهقاً، أما اليوم فيجب أن يكون البيان الفعال لرسالة المؤسسة عنصراً مهماً جداً في أي برنامج لأخلاقيات الإدارة والحوكمة الرشيدة للشركات. قد يكون البيان الفعال للرسالة أحد الأصول العظيمة للمؤسسة والذي يسمح لها بتحقيق جميع أهدافها وأغراضها على نحو أفضل.

على الرغم من مرور سنين طويلة على أزمة جونسون آند جونسون تايلينول Johnson Tylenol & التي وقعت أوائل ثمانينيات القرن الماضي، فإنها لا تزال تقدم مثالاً جيداً على أهمية البيان القوي لمهمة أو رسالة المؤسسة والذي يعمل كبوصلة لتقديم التوجيه المناسب. تعد شركة جونسون آند جونسون، واحدة من كبار موردي المنتجات الطبية، حيث قامت بتصنيع دواء شائع مسكن للألم ويؤخذ بدون وصفة طبية يسمى تايلينول Tylenol. وقد كانت هذه الأدوية تباع وقتها في زجاجات تغلق من الأعلى بسدادة لولبية. وقد قام أحد الأشخاص القاطنين في منطقة شيكاغو بفتح عدة زجاجات من دواء تايلينول هذا، وقام بغش محتوياتها بإضافة مادة السيانيد إليها، وقام بوضع هذه الزجاجات محل زجاجات أخرى على رفوف المتجر. وقد توفي العديد من الأشخاص الذين قاموا بشراء هذا التايلينول الملوث في وقت لاحق نتيجة تعرضهم للتسمم. وقد أشارت التحقيقات التي أجريت على هذه الحالات بسرعة إلى جونسون آند جونسون والتايلينول الملوث بالسيانيد.

هذا الأمر برمته قد وضع شركة جونسون آند جونسون تحت وطأة ضغوط هائلة. فقد كانت الشركة تعلم تماماً أنها تمتلك عمليات قوية جداً ومعمولاً بها لضبط الجودة التي من شأنها أن تمنع حدوث مثل هذا التلوث السام داخل مرافق التصنيع الخاصة بها. وعلمت أيضاً أن المنتجات الملوثة قد ظهرت فقط في منطقة شيكاغو، في حين أن تايلينول كان موجوداً على رفوف المتاجر في جميع أنحاء العالم. إن عملية السحب الكلي للمنتج ستكون مكلفة للغاية. ومع ذلك، فإن شركة جونسون آند جونسون لم تقم بسلسلة طويلة من التحقيقات الداخلية وقد قامت بسرعة باتخاذ الإجراء الصحيح. وقامت بسحب كل منتجات تايلينول الخاصة بها من رفوف المتاجر في جميع أنحاء العالم، وبعد ذلك قامت بإعادة إصدارها لهم في عبوات مختومة بتصميم جديد. وعندما سُئلت الشركة لماذا قامت بإصدار مثل هذا القرار بسرعة والخاص بسحب المنتج بالكامل رغم تكلفته العالية جداً ورغم عدم وجود دليل على أنها كانت على خطأ، أفادت الشركة بأنه لم تكن هناك حاجة لتأخير القرار. إن توجه شركة جونسون آند جونسون ورسالتها قد أملت عليها ذلك القرار. إن توجه جونسون آند جونسون ينص وبشدة على أن المسؤولية الأولى للشركة هي توفير منتجات عالية الجودة لعملائها. ويمكن العثور على نص هذا التوجه على موقع الويب الخاص بشركة جونسون آند جونسون وهي مبينة في الشكل التوضيحي (٢٠-١). في وقت أزمة التايلينول، كان الجميع في شركة جونسون آند جونسون على علم بهذا التوجه، فقد تم نشر هذه التوجه على نطاق واسع في مرافق المؤسسة، ولم يكن هناك حاجة وقتها لاتخاذ قرار بذلك. إن هذا الأمر المؤسف برمته قد أبرز بالفعل أهمية وجود بيان قوي لمهمة أو رسالة المؤسسة.

يعد البيان القوي لرسالة الشركة عنصراً هاماً في أي مبادرة من مبادرات الأخلاقيات وحوكمة الشركات. وعلى الرغم من أن معظم الشركات لن تواجه أزمة في مستوى أزمة شركة جونسون آند جونسون مع تايلينول الملوثة التي حدثت في ثمانينيات القرن الماضي، فإن قواعد قوية من هذا النوع قد ساعدت بعض الشركات لتجنب الفضائح المحاسبية في السنوات الأخيرة بصورة أفضل، تلك الفضائح التي أدت إلى ظهور قانون ساربينز أوكسلي (SOx) كما وضعنا في الفصل الثاني من هذا الكتاب.

شكل توضيحي (٢٠-١)

توجه أو بيان مهمة جونسون آند جونسون

توجهنا (كما نشرت في JnJ.com)

نحن نؤمن أن مسؤوليتنا الأولى هم الأطباء والممرضات والمرضى حتى الأمهات والآباء والجميع غيرهم ممن يستخدمون منتجاتنا وخدماتنا. وفي سبيل تلبية احتياجاتهم فإن كل شيء نقوم به يجب أن يكون ذا جودة عالية. ويجب أن نسعى جاهدين وبصفة مستمرة لخفض تكاليفنا من أجل الحفاظ على أسعار معقولة. إن طلبات العملاء يجب تلبيةها بسرعة وبدقة، ويجب أن يكون لدى موردينا وموزعينا فرصة لتحقيق ربح عادل.

نحن مسؤولون عن موظفينا، الرجال والنساء الذين يعملون معنا في جميع أنحاء العالم. يجب أن يُنظر إلى كل فرد كإنسان، ويجب علينا احترام كرامتهم والاعتراف بفضلهم. يجب أن يكون لديهم شعور بالأمن في وظائفهم، والتعويض يجب أن يكون عادلاً ومناسباً، أجواء العمل نظيفة، ومنظمة وآمنة. يجب علينا أن نفكر في طرق لمساعدة موظفينا حتى يستطيعوا الوفاء بمسؤولياتهم الأسرية. يجب أن يشعر الموظفون أنهم أحرار في تقديم الاقتراحات والشكاوى. يجب أن يكون هناك تكافؤ فرص للعمل والتنمية والتقدم لأولئك المؤهلين. يجب أن توفر الإدارة المختصة، ويجب أن تكون تصرفاتهم عادلة وأخلاقية.

نحن مسؤولون عن المجتمعات التي نعيش ونعمل فيها والمجتمع الدولي أيضاً. يجب أن نكون مواطنين صالحين - ندعم الأعمال الصالحة والجمعيات الخيرية ونتحمل نصيبنا العادل من الضرائب. يجب علينا أن نشجع التحسينات المدنية وتحسين الصحة والتعليم، ويجب أن نُبقي على الممتلكات المصرح لنا باستخدامها في حالة جيدة، نحمي البيئة والموارد الطبيعية.

مسؤوليتنا النهائية تكون تجاه أصحاب المصلحة لدينا. العمل يجب أن يجني ربحاً سليماً. لا بد لنا من تجربة أفكار جديدة. يجب أن يتم إجراء البحوث بشأن ابتكار برامج متطورة ودفع ثمن الأخطاء. يجب شراء المعدات الجديدة وإطلاق الوسائل الجديدة المتوفرة والمنتجات الجديدة. يجب إنشاء الاحتياطات لتغطية أوقات العسر. عندما نعمل وفقاً لهذه المبادئ، ينبغي أن يحقق أصحاب المصلحة عائداً عادلاً.

المصدر: جونسون آند جونسون.

يتعين على إدارة المؤسسة القيام بتقييم أي بيان ممكن أن يكون موجوداً اليوم لرسالة المؤسسة أو النظر في صياغته وإطلاق بيان آخر جديد إذا لزم الأمر. وإذا كان هناك موظفون أو غيرهم من أصحاب المصلحة ليسوا على علم بوجود أي بيان خاص بمهمة الشركة أو إذا كانوا ينظرون إليه بشيء من السخرية، فإن هناك حاجة إلى إعادة النظر في تلك الوثيقة ومراجعتها. تجد غالباً أن الضرر الناتج عن بيان الرسالة السيء الصياغة يتجاوز نفعه، بل ويؤدي إلى ظهور أعضاء في المنظمة ممن يقاومون التغيير يعبرون عن سخريتهم وعدم سعادتهم حيال ذلك. إذا لم يكن لدى المؤسسة أي بيان للمهمة أو القيم، فقد يكون هناك قيمة كبيرة في تكوين فريق يقوم بوضع بيان يعكس القيم والمقاصد العامة للمؤسسة. إذا تعرض البيان الحالي لمهمة المؤسسة إلى التهكم أو السخرية من خلال استبيانات استقصاء آراء أصحاب المصالح، إذاً فقد حان الوقت لصياغة وتنقيح هذا البيان بعناية. من ناحية أخرى، إذا تم تعميمه دون أي تحضيرات، فمن الممكن أن يُنظر إليه بالمزيد من التهكم. يعد البيان الجيد لمهمة المؤسسة أيضاً بمثابة نقطة انطلاق جيدة لرسالة "النعمة السائدة" لشركات اليوم، كما سبق مناقشته في الفصل الثاني من هذا الكتاب.

إن البيان الجيد لمهمة المؤسسة يجب أن يؤدي إلى تقارير إيجابية عن الشركة. كما ينبغي أن يلهم وبكل أمل أعضاء المنظمة لتسخير طاقاتهم وحماسهم وزيادة التزامهم لتحقيق الأهداف والغايات. إن الفكرة الأساسية هي إيجاد الشعور بالهدف والاتجاه الذي سوف تتم مشاركته في جميع أنحاء المؤسسة. وبالعودة مرة أخرى بالزمن قبل عدة سنوات، فقد يكون أحد أفضل الأمثلة على بيان المهمة هو ما عبر عنه الرئيس الأمريكي جون ف. كينيدي John F. Kennedy في أوائل ستينيات القرن الماضي:

"يتوجب على هذه الأمة أن تتفرغ تماماً لتحقيق الهدف، قبل انقضاء هذا العقد، بهبوط الإنسان على القمر وعودته إلى الأرض سالماً".

فقد قامت تلك الكلمات البسيطة بوصف المهمة والرؤية أفضل بكثير من وثيقة ضخمة تحتوي على العديد من الصفحات. وهي تسمى أحياناً بيانات القيم أو العقائد (التوجهات)، ويمكن أيضاً العثور على تلك البيانات في التقارير السنوية للعديد من المؤسسات. بعضها طويل، والبعض الآخر يبدو قصيراً بدرجة ملحوظة. فالبيان الأفضل هو ذلك الذي يُكتب

بأسلوب قريب من صياغة التوجه الخاص بجونسون آند جونسون أو بيان الهبوط على سطح القمر وفق أسلوب صياغتهم.

بمجرد أن تقوم المؤسسة بوضع بيان جديد للمهمة أو الرسالة أو تقوم بتنقيح بيان مهمة موجود، فإنه يجب تعميمه على كل أعضاء المؤسسة مع مستوى جيد من الدعاية. ومن خلال استخدام نهج النعمة السائدة، فإنه يتعين على كبار المديرين شرح أسباب البيان الجديد للمهمة ومدى أهميته بالنسبة للمؤسسة. ويجب نشره في لوحات إعلانات المؤسسة وفي التقرير السنوي وفي غيرها من الأماكن لتشجيع جميع أصحاب المصلحة على فهمه وقبوله. يجب ألا يعمل بيان المهمة بشكل منفصل، فهناك حاجة إلى سلسلة من الخطوات الأساسية الأخرى لبناء إدارة فعالة للامتثال والأخلاقيات، بدءاً من الدراسات الاستقصائية وغيرها من الآليات.

مدونة قواعد السلوك للمؤسسة:

في الوقت الذي يُعد فيه البيان القوي والفعال لمهمة الشركة عنصراً أساسياً في الهيكل العام لحوكمة الشركات، تعمل مدونة قواعد السلوك على توفير قواعد الدعم اللازمة لأصحاب المصلحة في المؤسسة. لقد كانت هذه القواعد شائعة في الشركات الكبرى لسنوات عديدة، ويطالب قانون SOX اليوم الشركات بوضع مدونة أخلاقيات لكبار المسؤولين الماليين. وبما أنه قد تم فرض هذه المدونة من قبل قانون SOX، فبإمكان جميع الشركات أن تستفيد من مدونة قواعد السلوك التي تشمل جميع أصحاب المصلحة. وعلى الرغم من أن قانون SOX يستخدم تعبير "مدونة أخلاقيات المهنة"، فإننا نشير إليها هنا باسمها الذي قد يكون أكثر شيوعاً وهو مدونة قواعد السلوك المهني للمؤسسة.

يجب على المؤسسة اليوم أن تضع وتطبق مدونة لقواعد السلوك المهني تشمل مجموعة مناسبة من القواعد الأخلاقية وقواعد العمل والقواعد القانونية لجميع أصحاب المصلحة في المؤسسة، متضمناً ذلك الإدارة العليا وجميع العاملين والمشرفين وأكبر فئة من أصحاب المصلحة بها. يجب أن تقوم الإدارة العليا للمؤسسة بتكوين فريق مكون من أعضاء العمليات التشغيلية للوحدات والمديرين الماليين وممثلين عن الرقابة الداخلية وضمان الجودة واتصالات الشركة والموارد البشرية وبالتأكيد الإدارة القانونية للشركة، وذلك لبناء أو

إعادة بناء مدونة فعالة لقواعد السلوك المهني والتي تُشجع الممارسات الأخلاقية للأعمال في جميع أنحاء المؤسسة.

المحتويات: ماذا يجب أن تكون رسالة المدونة؟

ينبغي أن تكون مدونة قواعد السلوك عبارة عن مجموعة من القواعد أو التوجيهات الواضحة التي لا لبس فيها ولا غموض والتي تحدد ما هو متوقع من أعضاء المؤسسة، سواء كان المتوقع من المسؤولين أم من الموظفين أو المقاولين أو البائعين أو أي من أصحاب المصالح الآخرين. وينبغي أن تستند المدونة إلى القيم والقضايا القانونية المحيطة بالمؤسسة. بمعنى أنه على الرغم من أن جميع المؤسسات يُفترض تبنيها مدونة قواعد السلوك المهني بما فيها محظورات ضد التمييز الجنسي والعنصري، فإننا نجد أن مقال الدفاع^(*) الذي يكون لديه العديد من القضايا المرتبطة بالقواعد المتعلقة بالتعاقدات سيحتفظ لديه بمدونة قواعد سلوك مهني مختلفة نوعاً ما عن تلك الخاصة بعملية تقديم الوجبات السريعة. ومع ذلك، يجب تطبيق أي مدونة بهذا الشكل على جميع أعضاء المؤسسة من أعلى مستوى وحتى موظف الأعمال الكتابية الذي يعمل بدوام جزئي. فعلى سبيل المثال، فإن مدونة قواعد السلوك التي تمنع رفع تقارير مالية خاطئة يلزم أن تكون هي المدونة نفسها، سواء تم توجيهها إلى المدير المالي فيما يخص التقارير المالية الخاطئة أم إلى الموظف الذي يعمل بدوام جزئي فيما يخص بطاقة الدوام الأسبوعي غير الصحيحة أو الاحتيالية.

إذا كانت المؤسسة لديها بالفعل مدونة لقواعد السلوك، فإنه ينبغي على إدارة المؤسسة النظر في تنقيحها أو تحديثها بحسب الحاجة. في كثير من الأحيان، نجد أنه تم وضع المدونات القديمة لتكون بالأساس قواعد لموظفي المستوى الأدنى، مع القليل من الاهتمام

(*) يسمى أيضاً المقاول الأمني (security contractor) وهي منظمة تجارية أو فرد يقدم منتجات أو خدمات لإدارة عسكرية أو استخباراتية تابعة للحكومة. وتشمل المنتجات عادة الطائرات العسكرية أو المدنية، والسفن، والمركبات، والأسلحة، والأنظمة الإلكترونية. ويمكن أن تشمل الخدمات اللوجستية والدعم التقني والتدريب ودعم الاتصالات والدعم الهندسي بالتعاون مع الحكومة. (المترجم).

الموجه للعديد من كبار أعضاء المؤسسة. إن المدونة الفعالة لقواعد السلوك المهني ينبغي توصيلها بطريقة من شأنها أن تُطبّق على جميع أصحاب المصلحة في المؤسسة، مع تركيز أكثر اليوم على كبار مسئولي المؤسسة. فبالتعاون مع كبار الموظفين في الإدارة ولجنة التدقيق، يجب على الفريق الإداري المحدد أن يقوم بفحص أي مدونة موجودة للسلوك المهني ليحدد ما إذا كانت قواعد وإرشاداتها لا تزال صالحة لحوكمة الشركات في عصر قانون SOX. سواء بالنسبة لعملية تنقيح المدونة الموجودة حالياً لقواعد السلوك المهني أو بالنسبة لتطوير مدونة جديدة، فإنه لا بد من تشكيل فريق مكون من شريحة إدارية منتقاة للقيام بهذه المهمة. بحيث يتعين على الفريق دراسة قضايا الأعمال التي تواجه المؤسسة ومن ثم القيام بصياغة مجموعة من قواعد المدونة القابلة للتطبيق على هذه المؤسسة اعتماداً على أعمالهم والقضايا ذات الصلة. ويجب أن تكون قواعد المدونة مكتوبة بطريقة واضحة بحيث يمكن فهم مثل هذه النقاط بسهولة من قبل الجميع. الشكل التوضيحي (٢٠-٢) يعرض أحد الأمثلة على موضوعات مدونة قواعد السلوك المهني. وعلى الرغم من أن هذه القائمة لا تنطبق على الجميع، فإن هذه الموضوعات تناسب العديد من المؤسسات الحديثة اليوم. فالنقطة الجوهرية هنا هي أن الرسائل المقدمة في المدونة يجب أن تكون واضحة ولا لبس فيها. وقد شارك مؤلف هذا الكتاب بشكل كبير في صياغة مدونة قواعد السلوك لإحدى الشركات الأمريكية الكبرى منذ عدة سنوات.

شكل توضيحي (٢٠-٢)

مثال لموضوعات مدونة قواعد السلوك

فيما يلي الموضوعات الموجودة في مدونة قواعد سلوك نموذجية لإحدى المؤسسات
<p>الأول: مقدمة:</p> <p>أ. الغرض من هذه المدونة لقواعد السلوك المهني: بيان عام حول خلفية هذه المدونة لقواعد السلوك.</p> <p>ب. التزامنا بالمعايير الأخلاقية القوية: إعادة ذكر بيان المهمة أو الرسالة إلى جانب الخطاب المطبوع من الرئيس التنفيذي.</p> <p>ج. أين تلتمس التوجيه أو الإرشاد: وصف لعملية الخط الساخن لأخلاقيات العمل في المؤسسة.</p> <p>د. الإبلاغ عن عدم الامتثال: إرشادات للمبلغين - كيف تُبلغ.</p> <p>هـ. مسؤوليتك عن الإقرار بالمدونة: وصف لعملية الإقرار بالمدونة.</p>
<p>الثاني: التعامل العادل:</p> <p>أ. ممارسة البيع لدينا: إرشادات للتعامل مع العملاء.</p> <p>ب. ممارسات الشراء لدينا: إرشادات وسياسات للتعامل مع البائعين.</p>
<p>الثالث: السلوك في مكان العمل</p> <p>أ. معايير تكافؤ فرص العمل: بيان التزام قوي.</p> <p>ب. مكان العمل والتحرش الجنسي: بيان التزام قوي بالقدر نفسه.</p> <p>ج. تعاطي المواد المخدرة وإساءة استخدام العقاقير: بيان السياسة العامة في هذا المجال.</p>
<p>الرابع: تضارب المصالح:</p> <p>أ. التوظيف الخارجي: فرض قيود على قبول طلبات التوظيف من المنافسين.</p> <p>ب. الاستثمارات الشخصية: القواعد المتعلقة باستخدام بيانات الشركة لاتخاذ قرارات تخص الاستثمار الشخصي.</p> <p>ج. الهدايا والفوائد الأخرى: القواعد المتعلقة بتلقي الرشاوى وتلقي هدايا في غير محلها.</p> <p>د. الموظفون السابقون: قوانين تحظر منح امتيازات للموظفين السابقين في مجال الأعمال.</p> <p>هـ. أفراد العائلة: قوانين حول إسناد أعمال لأفراد الأسرة، يخلق تضارباً في المصالح.</p>

الخامس: ممتلكات وسجلات الشركة:

- أ. أصول الشركة: بيان قوي حول مسؤولية الموظف عن حماية الأصول.
- ب. موارد نظم الحاسب الآلي: التوسع في بيان أصول الشركة ليعكس جميع الجوانب المتعلقة بـموارد نظم الحاسب الآلي.
- ج. استخدام اسم الشركة: هناك قاعدة، أن اسم الشركة يجب أن يتم استخدامه في التعاملات التجارية أو تعاملات الأعمال العادية فقط.
- د. سجلات الشركة: هناك قاعدة فيما يتعلق بمسؤولية الموظف عن سلامة السجلات.
- هـ. المعلومات السرية: قواعد حول أهمية الحفاظ على جميع معلومات الشركة السرية وعدم الكشف عنها لأطراف خارجية.
- و. خصوصية الموظف: بيان قوي حول أهمية الحفاظ على المعلومات الشخصية السرية للموظف وعدم الكشف عنها لأطراف خارجية وحتى للموظفين الآخرين.
- ز. منافع الشركة: يجب على الموظفين ألا يأخذوا من منافع الشركة ما لا يحق لهم.

السادس: الامتثال للقانون:

- أ. المعلومات الداخلية والتجارة الداخلية: هناك قاعدة قوية لحظر الأعمال التجارية داخل الشركة أو الاستفادة من المعلومات الداخلية.
- ب. المشاركات والأنشطة السياسية: هناك بيان قوي حول قواعد النشاط السياسي.
- ج. الرشوة والعمولات الخفية: هناك قاعدة صارمة بشأن قبول رشاي أو عمولات غير مشروعة.
- د. التعاملات التجارية الخارجية: القواعد المتعلقة بالتعامل مع وكلاء أجنبى بما يتماشى مع قانون ممارسات الفساد الأجنبية.
- هـ. السلامة في أماكن العمل: بيان حول سياسة الشركة لتتوافق مع قواعد^(١) OSHA .
- و. سلامة المنتج: بيان عن التزام الشركة بسلامة المنتجات.
- ز. الحماية البيئية: هناك قاعدة فيما يتعلق بالتزام الشركة لتتوافق مع القوانين البيئية المعمول بها.

(١) تمثل كلمة OSHA الحروف الأولى من كلمة Occupational Safety & Health Administration وهي إدارة السلامة والصحة المهنية الأمريكية، وتعد المنظمة أو المؤسسة الأكبر على مستوى العالم في مجال السلامة والصحة المهنية فهي تختص بوضع معايير الحفاظ على السلامة والصحة المهنية للعاملين في جميع المجالات، وتهدف إلى ضمان بيئة عمل آمنة وصحية لكل العاملين كما تسهم بفاعلية في الحفاظ على الموارد البشرية ومن ثم رفع مستوى الجودة في المؤسسات. (المترجم).

والمثال التالي مقتطف من تلك المدونة لقواعد السلوك الخاصة بقسم أصول الشركة: إننا جميعاً نتحمل مسؤولية رعاية جميع أصول الشركة متضمناً ذلك المخزون والنقدية والموارد والمرافق وخدمات الموظفين الآخرين وموارد نظم الحاسب الآلي. فإذا كنت ترى أو تشتهبه في أن موظفاً آخر يسرق أو يشارك في أنشطة احتيالية أو غير ذلك مما لا يحمي أصول الشركة كما ينبغي، فربما عليك الإبلاغ عن هذه الأنشطة إلى مديرك أو إلى مكتب أخلاقيات العمل.

تعد هذه الكلمات مثلاً جيداً على نبرة وأسلوب المدونة الجيدة لقواعد السلوك. ويضع المسؤولية على من يتلقى المدونة ويحاول شرح القضايا بطريقة لا لبس فيها، ويقترح الاستجابات للأفعال المتوقعة.

بالإضافة إلى موضوعات وقواعد المدونة، فإن العديد من الشركات قد وجدت قيمة في إضافة مجموعة من الأسئلة والأجوبة لترافق النقاط الموجودة في المدونة، الأمر الذي يسمح لقارئ المدونة أن يفهم القضايا على نحو أفضل، وكذلك أنواع الأسئلة التي ربما كثير من الموظفين البسطاء قد يسألون عنها فيما يخص قاعدة المدونة. إن مفتاح الوصول لمجموعة واضحة من قواعد السلوك المهني هو أنها يجب أن تكون واضحة ومفهومة بالنسبة للجميع. وقد يُشكل ذلك تحدياً فعلياً للتعديل بالنسبة لفريق مدونة قواعد السلوك.

إننا لم نقم بإدراج عينة من مدونات قواعد السلوك في هذا الكتاب، وذلك نظراً لاختلاف مدونات قواعد السلوك المهني لدى كل مؤسسة تقريباً من حيث الأسلوب والشكل والحجم. فبعض الشركات تنشر وثائق مفصلة إلى حد ما، في حين أن البعض الآخر يحتوي على الأساسيات فقط. ومن المؤكد أن مدونات السلوك المهني بطبيعتها ليست أسراراً تجارية للشركة، وتسفر الدعوات الموجهة إلى مكتب الاستعلامات أو العلاقات العامة بالشركة عن القيام بتجميع نسخ من عينات مدونة قواعد السلوك المهني لديهم.

إن الشركات العالمية لديها مشكلة أخرى عند قيامها بوضع مدونة لقواعد السلوك. فعلى الرغم من أن الشركة قد يكون مقرها في الولايات المتحدة، فإن عملياتها التشغيلية الرئيسية قد تكون منتشرة في جميع أنحاء العالم في مكان وجود المديرين الرئيسيين والموظفين وأصحاب المصلحة الآخرين من الذين لا يستخدمون اللغة الإنجليزية لغة أساسية لهم. وعلى الرغم من أن التكاليف الإضافية تتمثل في الترجمة، فإنه لابد من التفكير في إنتاج

نسخ من مدونة قواعد السلوك على الأقل باللغات الرئيسية المستخدمة في عمليات الشركة. وإذا كان هناك العديد من المواقع ولكن بها أعداد قليلة من أصحاب المصالح الناطقين بلغة أجنبية، فإنه سيكون من المناسب وضع ملخص لمدونة قواعد السلوك الأساسية بكل لغة من اللغات المحلية. ومع ذلك، ينبغي أن تؤكد تلك الإصدارات المختصرة التوجيهات نفسها للاحتيال المالي الخاص بالبنية الموجهة نحو الخدمة (SOA) الواردة في مدونة قواعد السلوك الأساسية.

تبليغ أصحاب المصلحة بمدونة قواعد السلوك لضمان الامتثال بها:

يجب أن تكون مدونة قواعد السلوك للمؤسسة عبارة عن وثيقة حية. وستكون قيمتها قليلة إذا ما تم وضعها وتوصيلها إلى جميع أصحاب المصلحة بكثير من الضجة، ثم بعد ذلك تُحفظ في مكان بعيد وتُنسى. سواء بالنسبة لمدونة جديدة لقواعد السلوك أو لمدونة موجودة تم تنقيحها بإضافة مزيد من التعديلات عليها، فإنه يجب على المؤسسة بذل المزيد من الجهد لتوصيل نسخة من هذه المدونة لجميع العاملين وأصحاب المصلحة. وتعد هذه خطوة أولى جيدة سيكون من شأنها تقديم تلك النسخة الجديدة أو المنقحة من مدونة قواعد السلوك بشكل رسمي لكبار المسؤولين التنفيذيين في المؤسسة، وخصوصاً المسؤولين الماليين. كانت مدونات القواعد السلوكية في الماضي تلقى أحياناً قبولاً رمزياً فقط من مجموعة المسؤولين الكبار، مع شعورهم بأن تلك المدونات قد صُممت في الواقع للموظفين وليس لهم. إلا أن الفضائح المالية التي تم الإبلاغ عنها والتي أدت إلى سن قانون SOx في السنوات الأولى من هذا القرن قد أبرزت في الواقع هذا التناقض. فكل من شركة إنرون Enron وشركة ورلد كوم WorldCom،^(١) وهما الشركتان اللتان يتم الاستشهاد بهما كثيراً كـ "أفراد السوء" في عصر ما قبل سن قانون SOx، قد كانت لديهم مدونات كافية لقواعد السلوك. ومع ذلك، فإن مسئولي الشركات لديهم بدوا كأنهم شعروا بأن تلك القواعد لا يمكن أن تطبق عليهم.

ويمكن اعتبار المدير المالي السابق لشركة إنرون (Enron)، أندرو فاستو (Andrew Fastow)، واحداً من الأمثلة المثيرة للقلق على عدم قبول كبار المسؤولين في الشركة لمدونة القواعد السلوكية. ولأنه كان على علم بأنه سيخالف مدونة قواعد السلوك بالشركة باتباعه

بعض المخططات المحاسبية المشكوك فيها غير المدرجة في الميزانية العمومية، فقد لجأ إلى لجنة التدقيق الخاصة بشركة إنرون وطلب منهم التصويت رسمياً على إعفائه من مدونة قواعد السلوك! وقد قامت اللجنة بمنحه هذا الإعفاء، وكانت خطوة أخرى على طريق الفشل الذي سارت فيه شركة إنرون ووصلت إليه في نهاية المطاف.

يجب على كبار مديري المؤسسة أن يُقرروا رسمياً بأنهم قاموا بقراءة وفهم مدونة قواعد السلوك وبأنهم سيلتزمون بها. وبمساعدة الفريق الإداري الذي يقف خلف تلك المدونة، فإنه ينبغي على المؤسسة أن تقوم لاحقاً بتعميم مدونة قواعد السلوك وإيصالها إلى جميع أصحاب المصلحة في المؤسسة. وقد يتم ذلك على عدة مراحل، وذلك عن طريق إيصالها أولاً إلى المرافق المحلية أو الرئيسية، تليها الوحدات الأصغر، والمواقع الأجنبية، وغيرهم من أصحاب المصلحة. وبدلاً من أن تحتفظ المؤسسة بنسخة من مدونة القواعد السلوكية مع مستندات المرتبات، فإنه يجب عليها بذل الجهود لكي تعرض تلك المدونة بطريقة تجذب الأنظار نحوها.

يمكن إيصال المدونة الجديدة ونشرها من خلال وسائل مثل المؤتمرات الإلكترونية (Webinar) التي يقودها الرئيس التنفيذي أو الجلسات التدريبية أو وسائل أخرى لتوصيل أهميتها ومعناها. هذا بالإضافة إلى أساليب الاتصالات الخاصة التي يمكن استخدامها لإيصال المدونة لجماعات أخرى كالباعة أو المقاولين، ولكن ينبغي أن يكون هدف الشركة هو الحصول على اعتراف رسمي من كل أصحاب المصلحة بأنهم سوف يلتزمون بمدونة قواعد السلوك الخاصة بالمؤسسة. ويمكن تحقيق هذا عن طريق أحد نظم الإنترنت أو النظم الهاتفية حيث يُطلب من كل أصحاب المصلحة في المؤسسة الرد على هذه الأسئلة الثلاثة:

- ١- هل تلقيت وقرأت نسخة من مدونة قواعد السلوك؟ أجب بنعم أو لا.
- ٢- هل فهمت مضمون مدونة قواعد السلوك؟ الإجابة بنعم إذا فهمت هذه المدونة لقواعد السلوك أو الإجابة بلا إذا كان لديك أسئلة.
- ٣- هل توافق على الالتزام بالسياسات والمبادئ التوجيهية الموجودة في هذه المدونة لقواعد السلوك؟ الإجابة نعم إذا كنت توافق على الالتزام بما جاء في المدونة، والإجابة بلا إذا كنت لا توافق.

إن الفكرة بأكملها هي أن يُطلب من كل فرد سواء كان موظفاً أم صاحب مصلحة أن يُقر بقبول مدونة قواعد السلوك الخاصة بالمؤسسة. يجب أن تُسجل تلك الردود باستخدام إحدى أشكال قواعد البيانات الحاسوبية بحيث يُدرج فيها اسم الموظف وتاريخ مراجعته والقبول أو عدم القبول. يمكن التعامل مع أي قضية من القضايا الناشئة عن السؤال الثاني من خلال برنامج المبلغين عن المخالفات الذي سيتم وصفه لاحقاً. والفكرة هي أنه يتعين على الجميع - كل أصحاب المصلحة - أن يساهموا في مبدأ مدونة قواعد السلوك والموافقة على شروطها. وإذا رفض أحد الأشخاص قبول المدونة لأسباب محددة، فإنه يتعين على المشرفين أو غيرهم مناقشة هذه المسألة مع هذا الشخص للوصول في نهاية المطاف إلى اتفاق. إن الموقف النهائي هنا هو أن المؤسسة يجب أن تتوقع أن كل الموظفين متفقون على قبول مدونة قواعد السلوك للمؤسسة والالتزام بها. إن اتباع مدونة قواعد السلوك ما هو إلا واحد من قوانين العمل، وأن الامتناع أو التخلف المستمر عن الالتزام بهذه القواعد ينبغي أن يكون سبباً للإيقاف عن العمل وإنهائه.

إن الفكرة بأكملها والتي تكمن وراء شرط الحصول على الاعتراف بهذه المدونة هي تجنب أي عذر مستقبلاً من نوع "لم أكن أعرف أن ذلك كان قاعدة" وذلك عندما تُواجه بأن هناك انتهاك للمدونة. إنها لفكرة جيدة أن يتم تطبيق هذه العملية الخاصة بقبول المدونة بصفة سنوية أو على الأقل بعد أي تنقيح لوثيقة المدونة. كما ينبغي الاحتفاظ بملفات توثيق هذه الإقرارات بالمدونة بطريقة آمنة.

انتهاكات المدونة والإجراءات التصحيحية:

تلخص المدونة السلوكية مجموعة من القواعد للسلوكيات المتوقعة في المؤسسة، والتي تكون على شكل إرشادات وتوجيهات موجهة لجميع أصحاب المصلحة — المسؤولين الماليين وغيرهم كالموظفين في جميع المستويات والمقاولين والبائعين. فبالإضافة إلى عملية نشر مدونة قواعد السلوك الخاصة بالمؤسسة والحصول على قبول أصحاب المصلحة بالمدونة، فإن هناك حاجة إلى وجود آلية للإبلاغ عن انتهاكات المدونة للتحقيق والتعامل مع تلك الانتهاكات.

إن الهدف المنشود هو أنه إذا كانت المؤسسة تُصدر مدونة قوية لقواعد السلوك إلى جانب رسالة الرئيس التنفيذي عن أهمية الممارسات الأخلاقية الحميدة، فإنه من المتوقع أن يقوم جميع أصحاب المصلحة باتباع هذه القواعد. ومع ذلك، فإننا جميعاً نعلم أن البشر هم البشر، وسيكون هناك دائماً بعض الذين ينتهكون القواعد أو يحومون حول انتهاكها. لذلك تحتاج المؤسسة إلى إنشاء آلية تسمح لموظفي الشركة أو حتى من خارج الشركة (الغرباء) بالإبلاغ عن الانتهاكات المحتملة للمدونة بطريقة آمنة وسرية. يمكن التعامل مع الكثير من آليات الإبلاغ من خلال الخط الساخن للأخلاقيات أو المبلغين عن المخالفات كما سيتم مناقشته في القسم التالي. هناك انتهاكات أخرى محتملة يجب معالجتها على مستوى مختلف. فلنفترض أن هناك أحد المشرفين الرجال يُلمح بأن تقديم خدمات غير شرعية من قبل إحدى الموظفات سيكون وسيلة جيدة للتقدم في المؤسسة. فإن مدونة قواعد السلوك فيما يخص حظر التحرش الجنسي لن تقوم بالضرورة بإيقاف هذا المشرف، كما أن الموظفة لن تستطيع في كثير من الأحيان إبلاغ المدير المباشر لهذا المشرف عن هذا الانتهاك. لذا ينبغي وضع عملية لرفع بلاغات بجميع أنواع الانتهاكات الأخلاقية.

لا بد من دعم مدونة قواعد السلوك في المؤسسة بالإجراءات والردود المخطط لها والموثقة عن الانتهاكات. فعندما يتم الإبلاغ أو العثور على مخالفات أو انتهاكات كبيرة للمدونة، فلا بد من إجراء التحقيقات، واتخاذ الإجراءات المناسبة، بغض النظر عن مرتبة ومكانة أصحاب المصلحة في المؤسسة المسؤولين عن تلك الانتهاكات. فإذا كانت مدونة قواعد السلوك تمنع عملية نسخ البرمجيات — وهو ما يجب أن يكون — فإن العقوبات الموقعة على أحد العاملين في الطاقم التحليلي لإحدى مكاتب المبيعات البعيدة يجب أن تكون هي العقوبات نفسها التي تقع على أحد كبار المسؤولين العاملين في مجلس إدارة الشركة. في حال كان الاثنان قد قرأا الحظر ووافقا عليه، فإنه يجب أن تكون العقوبات الواقعة عليهما متماثلة. خلاف ذلك، قد يؤدي إلى خلق جو يبدو فيه أن هذه القواعد لا تطبق على الجميع بالوتيرة نفسها.

يمكن التعامل مع معظم الانتهاكات لمدونة قواعد سلوك من خلال الإجراءات العادية للموارد البشرية في المؤسسة والتي ربما تلجأ إلى عملية تقديم النصيحة أو البقاء تحت

المراقبة بالنسبة للانتهاك الأول للمدونة، والتي قد تؤدي إلى إنهاء الخدمة في حال تكرارها. كما يجب إبلاغ السلطات الخارجية عن الانتهاكات التي تتعلق بأمور يبدو كأنها دعاوى مدنية أو جرائم محتملة، ليخرج الأمر بذلك عن سلطة المؤسسة. إن الهدف العام هو أنه يجب أن يكون لدى المؤسسة عملية معمول بها لتشجيع جميع أصحاب المصلحة على اتباع الممارسات الأخلاقية الحميدة، كما هو محدد في مدونة قواعد السلوك، كما يجب توفير آلية ملائمة للتبليغ عن الانتهاكات واتخاذ الإجراءات والتدابير النظامية المناسبة إذا تطلب الأمر.

الحفاظ على سريان المدونة:

يوجد العديد من القواعد الأساسية للسلوكيات الأخلاقية الجيدة وأيضاً للمؤسسة، لا تتغير من سنة إلى أخرى. فالقاعدة الموضحة في المثال في (الشكل التوضيحي ٢٠-٢) عن حماية أصول الشركة، التي تم الاستشهاد بها قبل قليل، قد نصت على أن جميع أصحاب المصلحة يتحملون مسؤولية العناية والاهتمام بأصول المؤسسة التابعين لها، سواء كانت ممتلكات أم نقدية أو موارد حاسوبية أو غيرها. وهذا النوع من القواعد الأخلاقية لا يتغير مع مرور الوقت، في حين قد يتعرض غيرها من القواعد إلى التغيير نتيجة ظروف العمل وعوامل أخرى. وقد قام مؤلف هذا الكتاب بتولي إدارة التدقيق الداخلي لإحدى الشركات الكبيرة للبيع بالتجزئة - سنطلق عليها اسم الشركة أ - التي كانت تمتلك في الأساس مدونة لقواعد السلوك تمنع الموظفين من العمل لدى الجهات المنافسة. وقد كان ذلك مناسباً عندما كان يعمل بائع في أحد مراكز التسوق لصالح الشركة (أ) بدوام كامل. وفي عصرنا الحالي الذي يتميز بأن هناك الكثير من العمل يكون بدوام جزئي، فإنه من غير المناسب أن أقول لبائع يعمل في أحد مراكز التسوق بدوام جزئي إنه أو إنها لن تتمكن من العمل بدوام جزئي ملتجئ تجزئة آخر، ولنطلق عليها اسم الشركة (ب)، موجودة في مركز التسوق نفسه. لذا فقد تم هنا تغيير مدونة قواعد السلوك لتنص على أنه يجب أن يكون ولاء الموظف للشركة (أ) وليس للشركة (ب) فقط أثناء عمله في الشركة (أ).

يتعين على المؤسسات أن تقوم وبشكل دوري بمراجعة مدوناتها المنشورة للقواعد السلوكية، وأن يكون ذلك كل سنتين على الأقل للتأكد من أن الإرشادات لا تزال قابلة للتطبيق وسارية. إن التغييرات التي تتم على مدونة قواعد السلوك ينبغي ألا تعامل

باستخفاف. فإن أي تنقيح ينبغي أن يمر من خلال عملية الإعلان والتعميم نفسها التي تم استخدامها عند تقديم المدونات للمرة الأولى. ينبغي إيصال المدونة المنقحة لجميع أصحاب المصلحة إلى جانب شرح التغييرات مع المطالبة بقبول إعادة الإقرار، كما أسلفنا.

إن الموظفين الجدد وغيرهم من أصحاب المصلحة الملتحقين بالمؤسسة، يجب أن تُعرض عليهم مدونة قواعد السلوك الحالية، بالشرط نفسه وهو أن يقرؤوا ويقرروا بما جاء بالوثيقة. ويمكن مشاهدة الفيديو المنشور على الإنترنت لشرح وتعليم الموظفين الجدد كل ما يتعلق بمدونة قواعد السلوك والتزام المؤسسة بها. وسواء تم تعديل المدونة أم لا، فإنه ينبغي أيضاً أن يُطلب من جميع أصحاب المصلحة، بصفة دورية، أن يُقرروا من جديد بأنهم قد قرؤوا وسيواصلون الالتزام بالمدونة.

إن التعديل الجديد لمدونة قواعد السلوك والمطالبة بإعادة إقرار أصحاب المصلحة يمكن أن تكون مهمة مكلفة وتتطلب موارد مخصصة من المؤسسة من إدارة الأخلاقيات والموارد البشرية والتدقيق الداخلي، وغيرها. وتمشياً مع بيان المهمة أو الرسالة، فإنه يجب على المؤسسة أن تُبقي مدونة قواعد السلوك والمبادئ الداعمة لها أمام جميع أصحاب المصلحة في جميع الأوقات. ويمكن تحقيق ذلك من خلال إشارات مستمرة لمدونة قواعد السلوك مثل ملصقات لوحة الإعلانات في جميع المرافق أو أسئلة وأجوبة توجيهية في مطبوعات أو عروض تقديمية في دورات تدريبية للموظفين.

المبلغون عن المخالفات وإدارات الخط الساخن:

تعد عملية الإبلاغ عن المخالفات من العناصر الهامة في حوكمة الشركات. والمبلغ عن المخالفات هو الشخص الذي يخبر الرأي العام أو شخصاً ما في السلطة عن أنشطة مزعومة غير شريفة أو غير قانونية تحدث في إحدى الدوائر الحكومية أو مؤسسة خاصة أو عامة. قد يكون سوء السلوك المقصود هنا عبارة عن انتهاك لأحد القوانين أو القواعد أو اللوائح أو تهديداً مباشراً للمصلحة العامة، مثل الاحتيال أو الانتهاكات المتعلقة بالصحة والسلامة أو الفساد. قد يدلي المبلغون عن المخالفات بدعوايهم داخلياً لجهات التحقيق داخل المؤسسة، أو خارجياً لجهات رقابية أو جهات إنفاذ القانون أو لوسائل الإعلام أو المجموعات المعنية بهذه القضايا.

لقد كانت برامج المبلغين عن المخالفات لعدة سنوات تدور حول دعم قوانين التعاقد الاتحادية ولوائح الصحة والسلامة، وغيرها. كما هو مبين في الفصل الثاني من هذا الكتاب، فإن قانون SOx يقضي بأن تقوم لجان التدقيق للمؤسسة بوضع إجراءات من أجل "التعامل مع معلومات المبلغ عن المخالفات فيما يتعلق بمسائل المحاسبة أو التدقيق المشكوك فيها". وعندما تم تفعيل قانون SOx للمرة الأولى، كان هناك الكثير من التكهّنات بأن هذا البند الخاص بالمبلغ عن المخالفات في قانون SOx سيصبح بمثابة كابوس، متمثلاً في إقامة الدعاوى الجنائية على العديد من الشركات الأمريكية، من خلال تقدم العديد من الموظفين بطلبات للإبلاغ عن المخالفات. إلا أن هذا الأمر لم يحدث حتى الآن، وحتى وقت نشر هذا الكتاب كان هناك عدد قليل من الشكاوى المسجلة لمبلغين عن مخالفات فيما يتعلق بقانون SOx قد تم رفعها، إلى جانب عدد أقل من إجراءات تسوية عادلة. وقد ثبت أن العملية القانونية وسيلة صعبة لحل القضايا وتسويتها.

ومع ذلك، فإن المؤسسة بحاجة إلى معرفة دعاوى المبلغين عن المخالفات والتعامل معها باعتبارها عنصراً هاماً من عناصر حوكمة الشركات. كما يجب على المؤسسة إيجاد إدارة داخلية للدعم بحيث يمكن لأي أحد من أصحاب المصلحة أن يبلغ دون الإعلان عن هويته عن أي مخاوف يشتبه بها، كما يمكن أن يتوقع الإجراءات العلاجية المناسبة. وبناء على خبرتنا في إنشاء مثل هذه الإدارات لإحدى الشركات الأمريكية الكبرى، فإننا نطلق على هذا النوع من المرافق اسم الخط الساخن للأخلاقيات.

ينبغي أن تكون إدارة الخط الساخن للأخلاقيات في المؤسسة عبارة عن مرفق يعمل أربعاً وعشرين ساعة في اليوم سبعة أيام في الأسبوع ٧/٢٤ بحيث يتمكن أي من موظفي الشركة وأصحاب المصالح من الذين يلاحظون أي شكل من أشكال المخالفات من التبليغ عنها بشكل سري ودون الخوف من عمليات انتقامية منه. وقد يتم رفع هذا الأمر إلى المنظمة أو إلى السلطات التنظيمية. يجب ألا يكون هناك أي عمليات انتقامية ضد الموظف أو المبادرة باتخاذ إجراءات قانونية لاستعادة التعويضات. حيث يمكن لهذه الدعاوى الخاصة بالمبلغ عن المخالفات إلحاق أضرار جسيمة بسمعة المؤسسة وكذلك على وظائف المديرين المتهمين. وفي الوقت الذي تطلب فيه قواعد قانون SOx من لجنة التدقيق أن تقوم بإنشاء

مرفق خاص للتبليغ عن المخالفات، فإن الإدارات الأخرى في المؤسسة كإدارة الموارد البشرية والتدقيق الداخلي وأخلاقيات العمل في الواقع تكون بحاجة إلى إعادة الأمور إلى نصابها بشكل حقيقي.

يضع برنامج التبليغ عن المخالفات الذي أقره قانون SOX تحدياً أمام أعضاء لجنة التدقيق. فالعضو العادي للجنة التدقيق التابع لمجلس الإدارة قد يكون مطلعاً على الاحتياجات الخاصة للبرنامج الفعال للمبلغ عن المخالفات، ولكن من شبه المؤكد أنه لن يكون مطلعاً على العمليات اللازمة لإنشاء أحد هذه البرامج. ويمكن لمجموعات التدقيق الداخلي أو الموارد البشرية في معظم الأحيان أن تساعد لجنة التدقيق في وضع برنامج فعال للمبلغ عن المخالفات الذي يتوافق مع متطلبات قانون SOX. إن البرامج الفعالة الخاصة بالإبلاغ عن المخالفات تعد واحدة من تلك المفاهيم التي قد يكون سمع بها الكثير من المديرين التنفيذيين، ولكن استيعابهم لها قد لا يكون بالشكل الكافي. وتوفر الأقسام التالية مزيداً من المعلومات عن هذه البرامج.

القوانين الاتحادية الخاصة بالمبلغين عن المخالفات:

إن القوانين الاتحادية الخاصة بالمبلغين عن المخالفات بوزارة العمل الأمريكية U.S. Department of Labor (DOL) تدير وتفرض ما يزيد عن ٢٠٠ قانون من القوانين الاتحادية التي تغطي العديد من أنشطة الأعمال لنحو ١٠ ملايين من أرباب العمل و١٢٥ مليون عامل. تقتضي معظم قوانين العمل والسلامة العامة والعديد من القوانين البيئية حماية المبلغين عن المخالفات بالنسبة للموظفين الذين يبلغون عن انتهاكات القانون من قبل أرباب عملهم. وتُطبق قواعد قانون SOX الخاصة بالمبلغين عن المخالفات على جميع العاملين في المنظمات المسجلة في هيئة الأوراق المالية والبورصة الأمريكية، ويتعين على الشركات العامة أن تُولي اهتماماً خاصاً بحماية المبلغين عن المخالفات في الشركات التابعة لها. ويقتضي قانون SOX حماية المبلغين عن المخالفات من أصحاب المصلحة في الشركات المطروحة للتداول، مما لا يسمح لأي شركة عامة أو أي مسئول أو موظف أو مقاول أو وكيل في مثل هذه الشركات "أن يُقال أو تُخفض مرتبته أو يُهدد أو يتم إيقافه أو مضايقته، أو أي طريقة أخرى تنطوي على

تمييز ضد الموظف في شروط وأحكام العمل نتيجة أي عمل قانوني قام به الموظف". تطبق تلك القوانين التشريعية عندما يقوم أحد الموظفين بتقديم معلومات أو يساعد في التحقيقات التي تجريها الوكالة الفدرالية التنظيمية أو وكالات إنفاذ القانون أو الكونجرس أو موظفي الشركة عن أي سلوك قد "يعتقد الموظف بشكل معقول" أنه يشكل انتهاكاً لقوانين ولوائح هيئة الأوراق المالية والبورصة الأمريكية أو قوانين الاحتيال أو الملفات أو الإدلاء بالشهادة أو المشاركة فيها أو غير ذلك مما يساعد في الدعاوى - المعلقة أو على وشك أن تحفظ - التي تتعلق بأي انتهاك مزعوم. وبعبارة أخرى، فإن الموظف أو أصحاب المصلحة الذين يرصدون بعض المخالفات المالية وبعد ذلك يقومون بالإبلاغ عنها، تتم حمايتهم قانونياً أثناء التحقيق في هذا الأمر والبت فيه.

في معظم الحالات، نجد أن الأحكام الخاصة بالمبلغ عن المخالفات قد وضعت في المقام الأول لحماية الموظفين الذين يظنون بأنهم قد اكتشفوا بعض المخالفات وليس لزيادة الضوابط الداخلية للمنظمة. من الممكن أن تخضع جميع الإجراءات المتخذة من قبل شؤون الموظفين بحق الأشخاص المبلغين عن المخالفات مثل تخفيض المرتبة أو الإيقاف، لعقوبات قانونية بموجب هذا القانون. وعلى الرغم من عدم وجود العديد من التجارب المتعلقة بالمبلغ عن المخالفات المتعلقة بقانون SOX في الوقت الراهن، فإنه من المتوقع أن يقوم كل من هيئة الأوراق المالية والبورصة ووزارة العمل، وهما من الوكالات الفيدرالية على نطاق واسع، بحماية الموظفين المبلغين عن مخالفات المحاسبة والتدقيق. ويشير ذلك إلى أن الموظف أو صاحب المصلحة الذي يسجل شكوى للإبلاغ عن المخالفات سوف يكون محمياً حتى يتم حل هذه المسألة.

بموجب قانون SOX، تعد جريمة أن يقوم شخص "عن علم وبقصد الانتقام" بالتدخل في عمل أو كسب الرزق لأي شخص - المبلغ عن المخالفات - يزود مسئول إنفاذ القانون بأي معلومات صادقة تتعلق بارتكاب جريمة محتملة لانتهاك قانون SOX. فأي موظف يبلغ عن مخالفة ويواجه بسبب ذلك ممارسات سلبية في العمل فإنه من المحتمل أن يصبح بمثابة "شاهد إثبات محمي".

يقتضي قانون SOx أن تقوم لجان التدقيق بإنشاء عملية لتلقي ومعالجة الشكاوى الواردة بخصوص المحاسبة وضوابطها الداخلية أو أي أمور تخص عمليات التدقيق ومن أجل "رفع الموظفين لتلك الشكاوى بشكل سري وغير معلوم الهوية" فيما يتعلق بمسائل المحاسبة أو التدقيق المشكوك فيها. إن أصحاب المصلحة الذين يدركون أنهم لن يتعرضوا للفصل أو التمييز غير القانوني نظراً لعملهم بصفة مبلغين عن المخالفات، سيسعون إلى مد يد العون عن طريق تقديم الشكاوى إلى وزارة العمل أو البدء بإجراءات المحاكم الفيدرالية. أما الذي سيتضرر فإنه سيحتاج عادة إلى الحصول على المساعدة القانونية الآمنة للسعي إلى تقديم المساعدة، وقد تتطلب هذه العملية المزيد من الوقت والتكلفة بالنسبة لكل من المبلغ عن المخالفات والشركة التي اتُهمت بالمخالفة. فعلى سبيل المثال، ولضمان التغلب على الشكاوى المقدمة، يجب على الموظف قبل الذهاب إلى وزارة العمل أن يثبت بأن المبررات التمييزية كانت عاملاً أسهم في حدوث هذا الإجراء الوظيفي الظالم في شأنه. ومع ذلك، فإنه يتم رفض موضوع الشكاوى، إذا ما أثبت صاحب العمل "بالأدلة القاطعة" أنه كان سيتخذ الإجراء الوظيفي نفسه حتى في ظل غياب هذا النشاط المحمي.

ويحق للموظف صاحب الحق في مثل هذا الإجراء المطالبة بالتعويضات الكاملة، متضمناً ذلك إعادته إلى منصبه وإعادة الأجر مع الفائدة والتعويض عن تكاليف التقاضي وأتعاب المحاماة. ومما يزيد الأمور تعقيداً، أنه يمكن للمبلغ عن المخالفات المتضرر أن يقوم باتخاذ إجراءات على عدة جبهات، فقد يسعى لطلب الحماية بموجب القوانين الاتحادية (الفيدرالية) وقوانين الولاية، وكذلك بموجب أي ميثاق تفاوض جماعي في هذا الشأن. ويتعرض أرباب العمل لخطر مزدوج بسبب إجراءات المبلغ عن المخالفات، من خلال المسؤولية التي تفرضها أحكام قانون SOx وكذلك القوانين الاتحادية وقوانين الولاية بشأن الفصل غير المشروع وأسباب مماثلة للإجراء. أضف إلى ذلك أنه، يمكن للمبلغ عن المخالفات المتضرر السعي للحصول على تعويضات تأديبية من خلال إجراءات قضائية منفصلة.

إذا حكمنا من خلال الخبرات الإدارية والقضائية السابقة في مجال صناعات الطاقة النووية وشركات الطيران، فإن قوانين حماية المبلغ عن المخالفات يمكن أن تصبح حقول ألغام للشركات. فإذا كان الموظف يثير أي نوع من أنواع التأكيدات التي تثبت أعمالاً غير

قانونية في الأمور المحاسبية والتدقيقية، فإن المبلغ عن المخالفات يكون محمياً تماماً حتى يتم التحقيق في المسألة والحكم فيها. وسيكون هناك العديد من المحامين المستعدين والحريصين على مساعدة المبلغ عن المخالفات ورفع الدعاوى، ولا سيما ضد الشركات الكبرى ذات الإمكانيات المالية الكبيرة. وبالإضافة إلى ذلك، فإن مجموعة كبيرة من وزارة العمل والمحاكم السابقين حاضرون في هذا المجال لدعم العقوبات التنظيمية والعلاجات الشخصية. ومن منظور خبرة امتدت لأكثر من ٢٠ عاماً في مجال أنشطة المبلغ عن المخالفات التابعة لقانون SOx في الولايات المتحدة، ينبغي أن تسعى المنظمة المعنية إلى تحقيق توازن بين حقوق الموظفين في رفع مخاوف مبلغي المخالفات والقدرة على إدارة القوى العاملة. إن بيئة العمل الإيجابية تحتاج إلى أن يشعر الموظفون بالحرية في رفع مخاوفهم إلى الإدارة وإلى آليات فعالة للتعامل مع أية مخاوف يتم إثارتها. إن البرامج القوية المتعلقة بالأخلاقيات التي تمت مناقشتها في الأجزاء الأولى من هذا الفصل تعد مهمة لإيجاد بيئة نأمل بأن تحد من النشاطات التي تستدعي الإبلاغ عن المخالفات.

قواعد الإبلاغ عن المخالفات وضوابط المؤسسة:

باستخدام قواعد قانون SOx مثلاً على ذلك يمكن لأي موظف أو أي شخص آخر من أصحاب المصالح أن يصبح من المبلغين عن المخالفات، وذلك بالإبلاغ عن أي نشاط غير قانوني أو غير لائق في مجال المحاسبة والرقابة الداخلية والتدقيق. وينبغي أن تكون هذه العملية أكثر فاعلية عندما يكون المبلغ المحتمل عن المخالفات هو أحد أعضاء طاقم المحاسبة للشركة الذي يسمع عن خطط لبعض المعاملات الاحتيالية أو موظف يعمل في وحدة نائية لا يرتادها موظفو الشركة باستمرار، كوحدة التدقيق الداخلي. فقد صُممت قواعد الإبلاغ عن المخالفات لتشجيع أصحاب المصلحة للإبلاغ عن هذه الأفعال الاحتيالية أو غير المشروعة وتحمي إلى حد كبير الشخص الذي يبلغ عن تلك الأمور. وهذا يثير سلسلة من القضايا بشأن المدققين الداخليين ومراجعات التدقيق الداخلي خصوصاً.

إن الهدف من عملية التدقيق الداخلي التي تمت مناقشتها في الفصل التاسع عشر من هذا الكتاب، هو مراجعة واكتشاف مشاكل الرقابة الداخلية وقضايا التدقيق الداخلي. حيث يتم مراجعة نتائج التدقيق الداخلي مع الإدارة وتقديم في شكل تقرير رسمي حيث

يمكن للإدارة وضع الخطوط العريضة لخططها الرامية لاتخاذ إجراءات تصحيحية. من ناحية أخرى، ماذا لو اكتشف فريق التدقيق الداخلي أن هناك مسألة من المسائل المتعلقة بالأمور المحاسبية أو الرقابة الداخلية أو التدقيق لم تُبلغ بها الإدارة رسمياً في تقرير التدقيق؟ هل يستطيع أحد أعضاء فريق التدقيق الإبلاغ عن هذه المسألة بموجب الإجراءات الخاصة بالإبلاغ عن المخالفات؟ هل يمكن للمدقق الداخلي الذي يصادف مسألة تخص المحاسبة والرقابة الداخلية وأنها ليست جزءاً من عملية التدقيق المجدولة، أن يسلك مسار حماية المبلغ عن المخالفات للإبلاغ عن تلك المسألة؟ ماذا لو كان عضو من أعضاء فريق التدقيق الداخلي لا يؤدي أداء جيداً ويخشى إنهاء الخدمة؟ وهل يمكن لهذا المدقق بوضعه المهتز أن ينبش في بعض النتائج المحتملة التي ربما تكون معتمدة على أوراق عمل سابقة، ويقدم تقريراً بها إلى جهة خارج إدارة التدقيق ليحصل على الحماية الخاصة بالمبلغ عن المخالفات والأمن الوظيفي حتى يتم تسوية المسألة؟

من الواضح أن فريق التدقيق الداخلي يعد جزءاً من الإدارة، فالمدققون الداخليون يتحملون المسؤولية الأولى في الإبلاغ عن أي مسائل غير نزيهة أو غير قانونية تواجههم خلال عمليات التدقيق إلى إدارة التدقيق الداخلي للبت فيها. لا ينبغي لأعضاء فريق التدقيق الداخلي أن يحاولوا العمل بشكل مستقل بصفة مبلغين عن المخالفات في جزء من عمل التدقيق الداخلي. بل يجب على التدقيق الداخلي أن يضع سياسة واضحة تنص على أن أي أمور تخص المحاسبة أو الرقابة الداخلية أو التدقيق وتتم مواجهتها خلال مراجعة التدقيق المجدولة، يجب أن يتم توثيقها في أوراق العمل الخاصة بالتدقيق وإرسالها إلى إدارة التدقيق الداخلي للبت فيها. يتعين على كل من فريق التدقيق الداخلي وإدارات الأقسام أو الوحدات التي يتم تدقيقها؛ أن يفهموا أن الغرض من التدقيق الداخلي هو عدم السماح لفريق مترصد من مبلغين المخالفات بتفقد دفاتر وسجلات الإدارة. وأن يتم التحقيق في أي بند من البنود غير القانونية أو غير اللائقة والإبلاغ عنها من خلال العملية الطبيعية للتدقيق الداخلي.

قد تظهر حالة يكتشف فيها مدقق داخلي إسقاط إحدى المسائل المحاسبية أو المتعلقة بالرقابة الداخلية من عملية التدقيق، وربما يحدث ذلك في عملية يقوم بها المدقق الأول

لمراجعة أوراق عمل. فالمدقق الداخلي هو أول من يتحمل مسؤولية الحصول على قرار في هذا الشأن من إدارة التدقيق الداخلي حتى يصل الأمر إلى مدير التدقيق الداخلي أو لجنة التدقيق. وفي حال قيام المدقق الداخلي بتوثيق المسألة والتبليغ عنها بينما ترى إدارة التدقيق إسقاط أو تجاهل هذه المسألة، فإن المدقق الداخلي وبكل تأكيد يكون له بعد ذلك الحق وعليه المسؤولية في أن يبلغ عن هذه المسألة، وهو مفعم بالأمل، من خلال إدارة الخط الساخن للأخلاقيات الخاصة بالمؤسسة أو حتى من خلال هيئة الأوراق المالية والبورصة. وينبغي أن تكون إدارة التدقيق والعمليات الأخرى المعمول بها في المكان المناسب لمنع مثل هذه الحالة المُحِبطة للمدقق الداخلي الذي يقوم بالإبلاغ عن المخالفات.

إطلاق إدارة الخط الساخن للأخلاقيات في المؤسسة:

قامت العديد من المؤسسات اليوم بإنشاء إدارات الخط الساخن للأخلاقيات. ويحتوي معظمها على وسائل سرية لخط الهاتف تدار من خلال قسم الأخلاقيات أو الموارد البشرية أو مقدم خدمات مستقل. إن عمليات الهاتف المجاني هذه، التي تعمل عادة على أساس ٧/٢٤، تسمح لأي موظف أو صاحب مصلحة بالاتصال بشكل سري ودون ذكر الاسم وطرح سؤال أو الإبلاغ عن مصدر قلق، أو "يطلق الصافرة" على مسألة ما. تتمثل فكرة توفير مرفق مستقل في أن يتمكن جميع أصحاب المصلحة من طرح الأسئلة أو الإبلاغ عن المخالفات المحتملة على أي مستوى. هذه الإدارات ليست مطلوبة من الناحية القانونية، ولكنها وسائل تمكن الموظفين أو غيرهم من أصحاب المصلحة في أكبر المؤسسات من طرح الأسئلة أو الإبلاغ عن تصرفات خاطئة محتملة أو طلب المشورة. قد تكون القضايا المبلغ عنها عبارة عن ادعاءات تتعلق بسرقة ممتلكات الشركة أو شكاوى من الموارد البشرية، أو لمجرد الاستفسار عن القضايا المثيرة للقلق. في معظم الحالات، سيقوم عامل الهاتف بأخذ جميع المعلومات اللازمة، وطرح أسئلة عند الحاجة، ومن ثم يقوم بتمرير الحادثة المبلغ بشأنها إلى السلطة المختصة للتحقيق والبت فيها. ويقوم الموظف المختص في إدارة الخط الساخن عادة بتخصيص رقم محدد للمسألة المبلغ عنها، ومن ثم فإن المتصل يستطيع أن يتحقق من الحكم في وقت لاحق.

تم تأسيس الخطوط الساخنة للموظفين في العديد من المنظمات الكبيرة بداية من منتصف التسعينيات من القرن الماضي. يكون الموظفون المخضرمون في الموارد البشرية في الغالب هم المشغلين المناسبين لتمتعهم بمهارات خاصة للرد على المسائل المتعلقة بالموارد البشرية، كالمعاملات والإجراءات الخاصة بأماكن العمل. أينما كانت أماكن ارتكاب المخالفات، فإنه يتم تحويل الحالة المسجلة إلى جهات أخرى كالإدارة القانونية مثلاً للتحقيق فيها. في بعض الأحيان نجد أن هذه الخطوط الساخنة قد تحولت إلى ما هو أكثر قليلاً من مجرد خطوط للتبليغ عن المخالفات، حيث استخدمت للتبليغ عن العديد من المشاكل والمخالفات الطفيفة إلا أنها كانت بشكل عام ناجحة جداً.

وعلى الرغم من أنه تم تأسيس العديد من إدارات الخط الساخن للأخلاقيات والسلوكيات للرد على استفسارات الموظفين وتقديم بعض النصائح والإرشادات والتحقيق في الحوادث المبلغ عنها بشكل إرضائي مناسب، فإنه باستخدام المبدأ نفسه نجد أن المرفق المنشأ بالفعل لبرنامج المبلغين عن المخالفات الخاص بقانون SOX يضع المزيد من الضوابط والمسؤوليات الجديدة على عاتق هذه الإدارة. وعلى الرغم من أن العديد من جوانب المساعدة الودية للخط الساخن للأخلاقيات يمكن أن تظل مطبقة، فإن القوانين الاتحادية للإبلاغ عن المخالفات تتطلب عمليات ذات طابع رسمي أكبر من ذلك بكثير، ولا سيما في مجالات مثل السرية والوثائق المطلوبة لكافة السجلات، والمعالجة الفعالة لأي تحقيقات. وبالإضافة إلى ذلك، فإن الموظف الذي يتم استدعاؤه في ادعاءات تدرج تحت بند الإبلاغ عن المخالفات التابع لقانون SOX يكون محمياً قانونياً من أي اتهامات مضادة في المستقبل. في بعض الحالات، نجد أنه لا بد من حماية الموظف المبلغ عن المخالفات بحيث لا يمكن أن تكون هناك أية إجراءات من أي نوع موجهة إليه من قبل صاحب العمل حتى يتم البت في هذه المزاعم أو الادعاءات. ومع ذلك، فمن أجل إنشاء مرفق خاص بالإبلاغ عن المخالفات في المؤسسة، لا بد من تعزيز الإجراءات الرقابية في جميع مرافق الخطوط الساخنة للأخلاقيات والسلوكيات التي تم إنشاؤها لهذا الغرض. الشكل التوضيحي (٢٠-٣) يحتوي على مبادئ توجيهية لإعداد برنامج للخط الساخن للأخلاقيات يخدم أيضاً مرفق الإبلاغ عن المخالفات في الشركة.

شكل توضيحي (٢٠-٣)

المبادئ التوجيهية لإعداد مركز اتصال للإبلاغ عن المخالفات

- إنشاء خطوط هاتف مستقلة - يفضل أن تكون مجانية - بريد إلكتروني آمن للمرفق. يجب ألا تمر هذه الخطوط من خلال لوحات التوزيع الأخرى للشركة.
- تدريب جميع العاملين في المرفق على الأحكام الأساسية للقواعد الاتحادية الخاصة بالإبلاغ عن المخالفات. وكذلك وضع النصوص بحيث يسهل على المتصلين طرح نفس الأسئلة العامة.
- الإعلان عن المرفق والترويج له وتعزيزه في جميع أنحاء المؤسسة مع التأكيد على الإبلاغ عن كل الوقائع، وسوف يكون المتصل قادراً على التحقق من الحالة وسيتم التعامل مع جميع المتصلين دون السؤال عن هويتهم، كما لن يكون هناك اتهامات مضادة بسبب ما يقوم به المتصل.
- تنفيذ نموذج تسجيل لتسجيل جميع المكالمات. الاحتفاظ بتاريخ ووقت المكالمات، واسم المتصل أو هويته، وتفاصيل البلاغ.
- إنشاء عملية للتوجيه والتخلص بحيث يمكن تحديد حالة من لديه معلومات المكالمات وحالة أي تحقيق.
- إنشاء قاعدة بيانات آمنة لجميع بيانات المبلغ عن المخالفات مع حماية مناسبة من خلال كلمة مرور.
- العمل مع الموارد البشرية، ووضع إجراءات لحماية تامة من الاتهامات من أي نوع لأي مبلغ غير أن هذه الحماية تكون غير معلومة.
- وضع عملية لتصفية كل المكالمات التي تخص المبلغ عن المخالفات، وتوثيق جميع الإجراءات، إن وجدت.

إن وجود مرفق خاص للخط الساخن والتبليغ عن المخالفات الأخلاقية ستكون قيمته محدودة ما لم يتم إيصاله و"بيعه" لجميع أعضاء المؤسسة. وهناك طريقة جيدة لإطلاق هذه العمليات من البداية وهي عن طريق مدونة قواعد السلوك التي نوقشت سابقاً. حتى إن كان قد تم إطلاق هذا الخط الساخن بالفعل، يلزم إخطار الجميع بحقيقة أن هذا الخط يمكن أن يستخدمه أي شخص من مبلغي مخالفات محتملة تخص البنية الموجهة نحو الخدمة. ويجب أن يكون الهدف هو التحقيق في جميع المكالمات والحل الفوري لها - وخصوصاً المكالمات الخاصة بالإبلاغ عن المخالفات - داخلياً لتجنب المحققين والمحامين الخارجيين.

إطلاق برنامج أخلاقيات العمل وتحسين ممارسات الحوكمة المؤسسية:

إن برنامج الأخلاقيات القوي، المستند إلى بيان مهمة ومدونة قواعد سلوكية ذات معنى، يعد عنصراً أساسياً لأي برنامج شامل لحوكمة المؤسسة. إن الفضائح المحاسبية التي أدت إلى ظهور قانون SOX في السنوات الأولى من هذا القرن، كانت في أغلب الأحيان عبارة عن فضائح في المستويات العليا من المؤسسة، سواء كان ذلك بسبب تأمر أحد المسؤولين الماليين أو الرؤساء التنفيذيين الجشعين أم بسبب إحدى شركات المحاسبة التي لا تسمح بالاستفسار عن أي شيء. فقد قامت الفرق التنفيذية الموجودة في الشركات التي تعرضت لفضائح محاسبية بتأسيس قواعد لها الخاصة مع إيلاء القليل من الاهتمام لباقي المؤسسة.

إن برنامج الأخلاقيات القوي سوف يحسن من ممارسات حوكمة الشركات للمؤسسة بأكملها وليس فقط من ممارسات الأشخاص الموجودين في المكاتب التنفيذية. ينبغي النظر في الإجراءات الخمسة التالية على أنها جزء من إطلاق إستراتيجية فعالة للأخلاقيات والإبلاغ عن المخالفات للمؤسسة بأكملها:

١- **سياسة الشركة:** يجب أن يتم إصدار بيان سياسة المؤسسة من قبل الإدارة العليا لضمان تشجيع جميع أصحاب المصلحة، بأنه تقع على عاتقهم مسؤولية لفت انتباه الإدارة حول المخاوف المتعلقة بالممارسات المحاسبية والمالية. يجب على بيان السياسة أيضاً أن يؤكد أن الإدارة لن تتسامح مع الانتقام من الموظفين الذين يبلغون عن المخالفات. يمكن للسياسة أن تساعد في تعزيز عملية "الباب المفتوح" لمعالجة القضايا، التي، في النهاية، هو النهج الأكثر فاعلية في الإدارة.

٢- **برنامج خاص بمخاوف وشكوك الموظفين:** يجب وضع برنامج لاستقبال ومعالجة جميع المخاوف والشكوك المقدمة من قبل الموظفين بشكل سري وعدم الكشف عن هوياتهم. وينبغي أن يتضمن البرنامج الفعال لمخاوف الموظف:

- منسقاً مركزياً لمعالجة الشكوك والمخاوف والتحقيق فيها.
- ضوابط لضمان إجراء التحقيقات الكافية باستمرار، مع التوثيق السليم الذي يصف القرار الصادر بشأن تلك الشكوك.

- آلية التغذية الراجعة لتقديم المشورة للموظف في التصرف وإبلاغه بالحكم المتعلق بالمسألة المبلغ عنها.
- عملية تقييم دوري لفاعلية البرنامج.

٣- **تدريب المشرفين:** ينبغي إجراء دورات تدريبية لجميع مشرفي الصف الأول والمديرين الآخرين حول كيفية الاستجابة بفاعلية للشكوك والمخاوف المطروحة من قبل الموظفين. تتصاعد المشاكل في كثير من الأحيان بسبب سوء الفهم بين الموظف ومشرفه أو مشرفته. فمن الممكن أن تعود بعض حالات العنصرية والتحيز والمحسوبية إلى الطريقة التي يتعامل أو يعالج بها المشرف حالة معينة مع أحد الموظفين. ومن ثم هناك حاجة ماسة لتدريب فعال للمشرفين والمديرين على التفاصيل الدقيقة المرتبطة بالشكوك والمخاوف المحتملة لدى المبلغين عن المخالفات.

٤- **إرشادات للمقاولين:** نظراً لاحتمالية وقوع الشركات العامة في شباك الأعمال العنصرية أو التحيزية أو المحسوبية الناجمة عن المقاولين الرئيسيين والمقاولين الفرعيين وغيرهم من الوكلاء، لذا ينبغي وضع آليات خاصة معمول بها، كتضمنين شروط محددة في العقود لحماية الموظف.

٥- **استطلاع آراء الموظفين:** وينبغي أن تجري الشركات وبشكل دوري مسوحات للقوى العاملة لديها لتقييم الثقافة المؤسسية وقياس ما إذا كان لدى الموظفين الشعور بالحرية في إبداء مخاوفهم وشكوكهم.

سواء أكانت شركة كبيرة أم صغيرة، فجميعها الآن تخضع لقواعد ومتطلبات قانون SOx. إن العمليات الخاصة بالأخلاقيات والإبلاغ عن المخالفات التي تمت مناقشتها في هذا الفصل تعتبر من الأمور الهامة لتحقيق التوافق مع قانون SOx والوصول كذلك إلى حوكمة مؤسسية رشيدة.

ملاحظة:

١. لمزيد من المعلومات حول شركة إنرون، وشركة ورلد كوم والشركات الأخرى التي شاركت في سن قانون ساربينز-أوكسلي يمكن العثور عليها في العديد من مصادر الإنترنت وكذلك كتاب روبرت مولر، *Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL* (Hoboken, NJ: John Wiley & Sons, 2008).

الفصل الحادي والعشرون

تأثير حوسبة وسائل التواصل الاجتماعي

هناك العديد من الأنواع والأنماط الجديدة التي نمت في السنوات الأخيرة في تطبيقات ومفاهيم تقنية المعلومات، وقد رافق ذلك ظهور بعض التطبيقات الجديدة والهامة والقائمة على ما يعرف بنظم وسائل التواصل الاجتماعي Social Media Systems، التي جاءت بمسميات مثل فيسبوك وتويتر ولينكدإن وغيرها الكثير. فقد كانت هذه التطبيقات موجهة في البداية إلى المستخدمين المستقلين، لتتيح لهم إمكانية نشر الملاحظات والصور وغيرها من المواد المتعلقة برسائل الصداقة الشخصية على الإنترنت وبين الأصدقاء بشكل عام. وهناك العديد من الأمثلة على ذلك، كأن تقوم إحدى الطالبات بنشر صورتها وبعض تفاصيل الحفلة التي أقيمت في المدرسة الثانوية، أو أن يقوم آباء فرحون بنشر صور ومعلومات عن مولودهم الجديد. وتُعرف نظم وعمليات إرسال الرسائل هذه بصفة عامة بتطبيقات حوسبة وسائل التواصل الاجتماعي، فالعديد من رسائلهم تكون مختصرة جداً ويتم إرسالها عبر الرسائل النصية المتاحة على العديد من الهواتف الخلوية. تعد نظم التواصل الاجتماعي من الأدوات العظيمة، وقد فاقت شعبيتها شعبية البريد الإلكتروني المستخدم بكثرة في مجال الأعمال هذه الأيام، وذلك باعتراف وشهادة الجميع. ومن الطبيعي أن تتسبب تطبيقات حوسبة الشبكة الاجتماعية في كثير من الأحيان في إثارة بعض القضايا المتعلقة بحوكمة تقنية المعلومات عند استخدامها داخل بيئات عمل المؤسسات.

ليس الهدف من هذا الفصل تقديم إرشادات تفصيلية عن استخدام تلك النظم أو التطبيقات الخاصة بالحوسبة الاجتماعية أو عن جوانبها التقنية، لكن الهدف هو مناقشة قضايا حوكمة تقنية المعلومات عندما تتعرض المؤسسة التي تسمح بحرية استخدام تلك النظم أو حتى تثبيتها لقضايا متعلقة بحوكمة الحوسبة الاجتماعية والرقابة الداخلية. قد تكون هذه النظم جزءاً رسمياً أو غير رسمي من البنية التحتية لتقنية المعلومات في العديد من المؤسسات اليوم، لذا يتعين على مديري المؤسسات أن يستفيدوا من بعض المزايا الإيجابية التي يمكن الحصول عليها من استخدام نظم وسائل التواصل الاجتماعي.

كما يجب عليهم أيضاً أن يدركوا أن نظم وعمليات تقنية المعلومات الخاصة بوسائل التواصل الاجتماعي قد تشكل بعض المخاطر المرتبطة بحوكمة تقنية المعلومات للمؤسسات الموجودة في الوقت الحالي.

ما المقصود بحوسبة وسائل التواصل الاجتماعي؟

إن تطبيق أو نظام التواصل الاجتماعي عبارة عن موقع خدمة أو منصة أو موقع تقني على شبكة الإنترنت يركز على بناء شبكات أو علاقات بين مجموعات من الأشخاص أو المستخدمين الذين يتشاركون الاهتمامات أو الأنشطة نفسها. قبل سنوات ليست بالبعيدة كان مفهوم تقنية المعلومات الخاص بنظام التواصل الاجتماعي غير معروف. إن مثل هذا النظام للتواصل الاجتماعي لديه العديد من الميزات والمخاطر في بعض الأحيان بشكل أكبر من النظام التقليدي للبريد الإلكتروني الذي يتم من خلاله تعريف كل مستخدم على الشبكة من خلال عنوان البريد الإلكتروني الخاص به دون الحاجة إلى المزيد من المعلومات عن المشترك. في حين على الجانب الآخر، يقوم الأشخاص الذين يتشاركون الاهتمامات والروابط بتسجيل الدخول إلى أحد النظم الخاصة بالتواصل الاجتماعي، وذلك من خلال عمل بطاقة دعوة أو توماتيكية خاصة بهم، أو من خلال تقديم لمحة مختصرة عن سيرة حياة المشترك. يحق لأعضاء الشبكة القيام بنشر صورهم أو معلومات عن سيرهم الذاتية، أو تعليقات عن أنشطتهم وأسرهم، أو في بعض الأحيان نشر آرائهم السياسية أو غيرها من المواد. تعتبر جميع خدمات وسائل التواصل الاجتماعي تقريباً عبارة عن تطبيقات تعمل على شبكة الويب، وتسمح للمستخدمين بالتفاعل عبر شبكة الإنترنت أو من خلال البريد الإلكتروني أو الوسائل الخاصة بإرسال الرسائل النصية الفورية. كما تسمح مواقع التواصل الاجتماعي للمستخدمين بتبادل الأفكار والأنشطة والأحداث والاهتمامات من خلال شبكاتهم الشخصية.

في الحقيقة، إن تطبيقات تقنية المعلومات الخاصة بوسائل التواصل الاجتماعي كانت قد ظهرت وبشكل جيد قبل عصرنا الحالي الذي يشهد حالياً انتشاراً واسعاً لشبكة الإنترنت وحتى قبل ظهور الحاسبات الشخصية المحمولة. وفيما يلي بعض الاتجاهات الرئيسية في تطوير حوسبة وسائل التواصل الاجتماعي منذ بدايتها وحتى الآن:

• ١٩٧٨-١٩٨٩: تطبيقات من نوع واحد إلى قليل: في الأيام الأولى لظهور أجهزة الحاسبات الشخصية (على سبيل المثال، Apple II أو IBM PC)، كان التطبيق الأول المتعارف عليه لوسائل التواصل الاجتماعي يسمى نظام لوحة الإعلانات أو نظام لوحة النشرة المحوسب (Computerized Bulletin Board System (CBBS، والذي أنشئ في شهر فبراير من عام ١٩٧٨ بواسطة وارد كريستنسن Ward Christensen، الذي كان يعمل في شركة IBM^(١). وقد تم استخدام هذا النظام من قبل مجموعة من مطوري البرمجيات في شركة IBM ليقوموا بمشاركة الرسائل التي تتعلق بأوقات وأماكن الاجتماعات، وذلك لتقليص الوقت المهدر في المكالمات الهاتفية. وربما كان هذا التطبيق هو المثال الأول للتطبيقات التفاعلية التي يتجاوز فيها حد الرسائل المرسلة نمط الواحد لواحد ليصل إلى نمط واحد إلى قليل.

في الحقيقة فإن شبكة الإنترنت لم تكن شائعة في ذلك الوقت، إلا أنه سرعان ما انتشرت آلاف من نظم لوحات الإعلانات CBBS، بمسميات مثل فيدوننت FidoNet في جميع أنحاء أمريكا الشمالية وغيرها من الأماكن، لتصبح أدوات مفيدة وذات شعبية متزايدة للاتصالات بين المستخدمين المتباعدين جغرافياً والذين كان بإمكانهم الوصول إلى هذه النظم من خلال أجهزة المودم الهاتفية.

• ١٩٩٠-١٩٩٤: نمو الإنترنت: في أوائل تسعينيات القرن الماضي، كان استخدام الإنترنت متاحاً بداية فقط للمؤسسات الحكومية والعسكرية والأكاديمية. فقد توجب على مؤلف هذا الكتاب، أثناء قيامه بتأليف كتابه الأول عن تدقيق تقنية المعلومات، أن يبحث عن أحد معارفه في إحدى الجامعات المحلية لمنحه إذناً كتابياً لإنشاء حساب إنترنت يسمح له بالوصول إلى بعض الوثائق الخاصة بتدقيق تقنية المعلومات. ولكن، سرعان ما ظهر العديد من تطبيقات الإنترنت التجارية القائمة على المستهلك بمسميات مثل بروديجي Prodigy وكومبيوسيرف CompuServe. وسرعان ما تحولت هذه الخدمات إلى مقدمي خدمات الإنترنت (Internet service providers (ISP كما كان يطلق عليها سابقاً في المدن الرئيسية في الولايات المتحدة.

وسرعان ما لاقى القبول الزائد للمستهلكين على الإنترنت تأييداً كبيراً من شركة أمريكا أون لاين AOL، وهي الشركة التي قامت بتسويق الإنترنت بقوة عن طريق نشر الملايين من أقراص الاشتراك الخاصة بها، حيث تمكن المشاركون من الوصول إلى الإنترنت، وإرسال رسائل البريد الإلكتروني، وشراء البضائع، والمشاركة في مفهوم جديد من منتديات الإنترنت. هذا بالإضافة إلى الفرصة التفاعلية للانضمام إلى المنتديات على الإنترنت وبث رسائل البريد الإلكتروني، كانت هذه التطبيقات هي الخطوات الأولى في التطبيقات التدريجية لوسائل التواصل الاجتماعي.

• ١٩٩٥-١٩٩٩: طفرة الدوت كوم: لقد شهد هذا العصر طفرة كبيرة في تقنيات الويب وأدوات الإنترنت. وقد اعتمدت معظم تلك التطبيقات الجديدة على المنتجات الاستهلاكية الجديدة وعلى عمليات التسويق. ولم يحدث في هذه الفترة أي تطور أو نمو في تطبيقات وسائل التواصل الاجتماعي يتجاوز حدود مواقع لوحة الإعلانات الموجودة.

فقد كان الاستثناء الوحيد في هذا العصر هو ظهور تطبيق SixDegrees.com، وهو من أوائل مواقع الويب الخاصة بالشبكات الاجتماعية، وقد استمر خلال الفترة ١٩٩٧-٢٠٠١، وقد تمت تسميته وفقاً للمفهوم "ست درجات من الانفصال"^(٢). وقد سمح هذا التطبيق للمستخدمين بإدراج الأصدقاء وأفراد الأسرة، والمعارف، كما سمح أيضاً للمتصلين الخارجيين بالانضمام إلى الموقع. وتمكن المستخدمون من إرسال رسائل ونشر الإعلانات والحوارات النقاشية للأشخاص الذين هم من الدرجة الأولى أو الثانية أو الثالثة بالنسبة لهم، كما تمكن المستخدمون من مشاهدة الروابط مع الأشخاص الآخرين الموجودين على الموقع. فقد كان هذا التطبيق واحداً من التطبيقات الأولى لمواقع الويب الخاصة بشبكة التواصل الاجتماعي بالنمط نفسه الذي نشاهده هذه الأيام.

• ٢٠٠٠-٢٠٠٤: نمو الاتجاه نحو وسائل التواصل الاجتماعي: على الرغم من أن المخاوف المتعلقة بقدوم العام ٢٠٠٠ Y2K لم تشكل أزمة بالحجم الذي كان متوقعاً، ومن انحسار الطفرة التي حدثت في الدوت كوم، فإن هناك العديد من تطبيقات وسائل التواصل الاجتماعي الجديدة قد أطلقت خلال هذه الفترة، منها ماي سبيس MySpace، وفيسبوك Facebook، وفريندستر Friendster، ولينكدإن LinkedIn وغيرها. وسوف نناقش بعضاً من هذه التطبيقات بمزيد من التفصيل في الأقسام التالية.

وقد تم استخدام العديد من هذه التطبيقات الجديدة على نطاق واسع من قبل أشخاص من داخل المنظمات المؤسسية ومن خارج التطبيقات الخاضعة لسلطة المؤسسة. وعلى الرغم من أنه كان هناك دائماً بعض الأصوات المرتفعة على نطاق ضيق، فإن تطبيقات وسائل التواصل الاجتماعي قد سمحت للناس بإنشاء المحتوى والمشاركة في التعليقات دون مشاركة المنظمة — وهو توجه هدام في غالب الأمر!

أثناء هذه الفترة تم إطلاق تطبيق آخر على منصة الإنترنت، وهو وورد WordPress، والذي سمح للأشخاص الذين ليس لديهم معرفة بالبرمجة ببناء وإطلاق مواقع المدونات الإلكترونية أو المذكرات الشخصية أو مواقع المحتوى. فباستخدام هذه الأداة، يمكن لأي شخص أن يقوم باستضافة مدونة إلكترونية على موقع المجال الذي يمتلكه أو تمتلكه ولها السيطرة الكاملة على تصميمه ومحتوياته بصورة أساسية. وقد كانت هذه خطوة كبيرة نحو الصحافة الشخصية.

• ٢٠٠٥-٢٠٠٩: استمرار نمو تطبيقات الشبكات الاجتماعية: استمر نمو وتطوير تطبيقات وسائل التواصل الاجتماعي، وذلك من خلال ظهور تطبيقات مثل يوتيوب Youtube، وهو موقع ويب خاص بتبادل ملفات الفيديو، حيث يمكن لأي شخص أن يقوم بنشر أي محتوى للفيديو. وقد ازدادت شعبية استخدام الهواتف الذكية بشكل كبير وملحوظ، في هذه الفترة، وأصبحت رائجة على نطاق واسع، ويمكن للمستخدم أن يحمل عليها مجموعة متنوعة من التطبيقات. ربما كان التطبيق الجديد والأكثر أهمية في وسائل التواصل الاجتماعي خلال هذه الحقبة هو تويتر Twitter، وهو تطبيق يستخدم للرسائل أو التعليقات الإلكترونية القصيرة، حيث يستطيع المستخدم أن يقوم بنشر رسائل تعتمد على المحتوى القصير ومتابعة الآخرين من خلال دفعات قصيرة من المعلومات. وسوف نقدم تويتر بمزيد من التفصيل في قسم لاحق.

• ٢٠١٠ وما بعدها: استمر نمو استخدامنا لتطبيقات الوسائل الاجتماعية في هذه الفترة، الأمر الذي تسبب في ظهور العديد من القضايا والمخاوف المتعلقة بحوكمة تقنية المعلومات في المؤسسات هذه الأيام. فعلى سبيل المثال، قد شهدت الأحداث العالمية خلال الأشهر الأولى من عام ٢٠١١ ما أطلق عليه شعبياً اسم الربيع العربي، حيث تم الإطاحة بالقادة

السياسيين المستبدين في كل من تونس ومصر وليبيا. وقد بدأت الاحتجاجات المناهضة للحكومة في كل دولة من تلك الدول بعد إجراء العديد من الاتصالات والحوارات عبر وسائل التواصل الاجتماعي بواسطة الفيسبوك وغيره من الوسائل الأخرى. فقد رأى الناس الأحداث التي أثارت غضبهم وقاموا بنشر تعليقاتهم وصورهم للآخرين، من الذين قاموا بنقلها لأشخاص آخرين. وكانت النتيجة هي تصاعد موجات من الاحتجاجات الشعبية التي سرعان ما أطاحت بتلك الحكومات.

وعلى الرغم من أن استخدام الناس لمثل هذه الوسائل الخاصة بالتواصل الاجتماعي "فيسبوك" للإطاحة بالحكومات الاستبدادية يعد واحداً من الأمثلة الحقيقية على السلطة القوية لتلك الوسائل، فإنها لا تزال تحمل بعض التحديات التي تتعرض لها المؤسسات هذه الأيام. فمن الممكن أن تشكل أدوات وخدمات وسائل التواصل الاجتماعي بعض التحديات بالنسبة لحوكمة تقنية المعلومات في المؤسسات هذه الأيام. فإن هذه النظم تعتبر جديدة بالنسبة للعديد من المؤسسات الحالية، ولا تستطيع تلك المؤسسات التي لا تزال تستخدم النظم والتطبيقات التقليدية لتقنية المعلومات أن تكون في المكانة التي تسمح لها بسهولة بتبني نظم وسائل التواصل الاجتماعي المفتوحة والمرنة. هذا بالإضافة إلى أنه سيكون الأشخاص العاملون في المؤسسة في الغالب عبارة عن مستخدمين يقومون باستخدام تطبيقاتهم الخاصة بحوسبة وسائل التواصل الاجتماعي بشكل شخصي. الأمر الذي من الممكن أن يثير بعض المشاكل المتعلقة بحوكمة تقنية المعلومات في حال لم تقم المؤسسة بوضع القواعد والإجراءات المناسبة التي تغطي العمليات التشغيلية لتلك الوسائل.

أمثلة على وسائل التواصل الاجتماعي:

ستتناول الأقسام التالية ثلاثة من أشهر تطبيقات وسائل التواصل الاجتماعي التي يختلف بعضها عن بعض كلياً (فيسبوك ولينكدإن وتويتر)، كما أنها ستتناول بعض القضايا المميزة الخاصة بالحوكمة المحيطة بكل تطبيق من هذه التطبيقات. لقد بدأ استخدام كل تطبيق من هذه التطبيقات بشكل شخصي، إلا أن الناس قاموا بنقله إلى أماكن العمل من خلال الاتصالات التي يجرونها على نظم الحواسيب المحمولة والهواتف الذكية الخاصة بهم.

فيسبوك Facebook:

فيسبوك هو أحد خدمات ومواقع الويب الخاصة بالتواصل الاجتماعي التي تم إطلاقها في شهر فبراير من عام ٢٠٠٤ من قبل مارك زوكربيرج Mark Zuckerberg وعدد من زملائه القاطنين معه في السكن الجامعي الخاص بجامعة هارفارد Harvard، وسيلة للتواصل وتبادل المعلومات بين زملائه من طلاب الجامعة. كان تطبيق الفيسبوك في البداية مقتصرًا فقط على طلاب جامعة هارفارد، ولكن سرعان ما امتد ليصل إلى الكليات الأخرى في منطقة بوسطن، ثم وصل إلى جامعة آيفي ليغ Ivy League، ثم جامعة ستانفورد Stanford. وقد أخذ فيسبوك تدريجياً في نيل دعم طلاب الجامعات الأخرى عن طريق السماع قبل أن ينتقل بعد ذلك ليصل إلى طلاب المدارس وغيرهم من المستخدمين. أصبح نظام فيسبوك هذه الأيام يحظى بشعبية كبيرة ويستخدم من قبل الكثير والكثير من الأشخاص في جميع أنحاء العالم. كما أنه حل محل البريد الإلكتروني كوسيلة للاتصال بين الأفراد بالنسبة للعديد من الأشخاص هذه الأيام.

أصبح عدد المستخدمين النشطين لنظام فيسبوك في أغسطس ٢٠١٢ يزيد عن ٩٥٠ مليون بعد أن كان يستخدم من قبل مستخدمين محدودين في السكن الجامعي عام ٢٠٠٤، وما زال عدد المستخدمين لهذا التطبيق في تزايد مستمر. وقد بدأت شركة فيسبوك العمل على أنها شركة خاصة إلا أنها أصبحت مؤخراً شركة عامة.

تكون البداية الأولى للأفراد المستخدمين لتطبيق فيسبوك ناتجة غالباً عن تحفيز من أحد الأشخاص، وهو عادة ما يكون صديقاً شخصياً، يقوم بإرسال رسالة بريد إلكتروني إليهم طالباً منهم أن يصبحوا أصدقاءه على فيسبوك. وبعد ذلك سيطلب من المستخدم الجديد بأن يقوم بإنشاء ملف شخصي، وإضافة مستخدمين آخرين كأصدقاء ليتبادلوا الرسائل والإشعارات التلقائية التي تنطلق عند تحديث ملفاتهم الشخصية. كما يمكن للمستخدمين الانضمام إلى مجموعات المستخدمين ذوي الاهتمام المشترك التي تم ترتيبها وتنظيمها من قبل مكان العمل أو المدرسة أو الكلية، أو غير ذلك من المعالم.

الانضمام إلى فيسبوك:

وبالنسبة لكثير من محترفي الأعمال الرفيعي المستوى، يعتبر فيسبوك أكثر من مجرد تطبيق تقنية معلومات. فهو في غالب الأمر مفهومٌ ربما يكون كبار محترفي الأعمال قد قرؤوا عنه، حتى وإن لاحظنا في كثير من الأحيان عدم فهم المدير التنفيذي نفسه لهذا النظام، والذي يتجاوز عادةً حدود التعليقات والأنشطة التي يقوم بتبادلها مع أبنائه وغيرهم من البارعين في تقنية المعلومات. وقد يكون هذا حقيقياً خصوصاً إذا كان لدى المرء أبناء يستخدمون ويفهمون نظام فيسبوك وهم في سن الجامعات أو المدارس الثانوية. فهناك ٦٠٪ من ملايين المستخدمين لفيسبوك هم دون سن ٣٥.

في كثير من الأحيان يشارك الشخص في فيسبوك للمرة الأولى من خلال تلقيه رسالة بريد إلكتروني من قبل أحد شركاء الأعمال أو الأقارب طالباً منه أي يصبح "صديقاً" له على فيسبوك. الشكل التوضيحي (٢١-١) يوضح الخطوات اللازمة لتسجيل الدخول إلى الفيسبوك. الفكرة هي أن الشخص يقوم بتسجيل الدخول بالاعتماد على الدعوة الأولية الموجهة إليه، ومن ثم يمكنه الاتصال بالآخرين الذين هم أيضاً مستخدمون لفيسبوك. يمكن للأصدقاء على فيسبوك الاتصال مع الآخرين بطريقة متتالية بصفة أصدقاء الأصدقاء، الذين يمكنهم الاتصال لإنشاء شبكة واسعة.

استخدام فيسبوك:

إن تطبيق فيسبوك أكثر بكثير من أن يكون مجرد بديل عن استخدام نظام البريد الإلكتروني، فهو يسمح لك بأن تقوم ببناء ملف شخصي خاص بك، ونشر أو إرسال الرسائل لكل شخص من الأشخاص الموجودين على قائمة الأصدقاء الخاصة بك، لتقوم بتقديم الشروحات للأنشطة التي تمارسها، ولتبادل الرسالة مع أصدقائك على الفيسبوك، والعديد من الأنشطة الأخرى. فقد تتشابه إلى حد ما هذه الرسائل سواء كانت نصية أم صوراً مع محتويات البريد الإلكتروني أو الرسائل النصية القصيرة المرسلة من خلال الهواتف الذكية. ومن المؤكد أن تلك الرسائل المرسلة في بيئة السكن الجامعي تكون عادة عبارة عن تعليقات وصور تتعلق بإحدى الحفلات أو الأحداث التي وقعت مؤخراً. وتكون في العادة مجرد

ملاحظات يتم إرسالها دون الحاجة للرد. ويمكن لمستخدم فيسبوك أن يقوم بإرسال مذكرة محددة أو سؤال إلى أي شخص أو لجميع الأشخاص الموجودين على قائمة أصدقائه. ويمكن عندئذ أن ترسل أو تُوجّه تلك الرسائل إلى غيرهم.

شكل توضيحي (٢١-١)

خطوات الانضمام لفيسبوك

الخطوة ١.	قم بزيارة موقع فيسبوك (www.facebook.com).
الخطوة ٢.	قم بإدخال اسمك بالكامل، عنوان بريد إلكتروني سليم، وتاريخ الميلاد. وبالإضافة إلى ذلك، ينبغي عليك إدخال أكبر قدر من المعلومات الشخصية وذلك عندما ترغب في نشرها على حسابك في فيسبوك في القسم "حول" About". وهذا قد يشمل عنوان العمل، والخلفية التعليمية، وأي مجال من المجالات العديدة الأخرى الخاصة بالاهتمامات الشخصية. يمكن للمرء أن يضع أيضاً صورة رقمية، أو صورة لأحد الزوجين والأسرة، وغيرها من المعلومات الشخصية في هذا المكان. يمكن لمستخدم جديد في فيسبوك أيضاً اختيار "لا شيء مما سبق" لتكون مجرد اسم مع قليل من المعلومات الشخصية.
الخطوة ٣.	اختر كلمة مرور خاصة بك. إدخال كلمة مرور يسهل تذكرها من ستة أحرف على الأقل.
الخطوة ٤.	أكمل اختيار التحقق من الصورة. حدد الكلمات أو الأرقام المعروضة واكتبهم.
الخطوة ٥.	اقرأ شروط الاستخدام وسياسة الخصوصية الخاصة بالفيسبوك. ضع علامة داخل المربع لتعبر عن موافقتك على شروط كل منهما.
الخطوة ٦.	انقر على زر "اشترك!" في أسفل الصفحة وانتظر إعادة توجيهه إلى صفحة الشكر لكم.
الخطوة ٧.	راجع صندوق البريد الإلكتروني الخاص بك وانقر على صفحة التأكيد من فيسبوك. فإنها سوف ترسل لك رابط التأكيد للتسجيل الخاص بك.

تستطيع منشورات الفيسبوك أن تعرض وصفاً تفصيلياً عن الحياة الشخصية لأحد الأشخاص ونشاطاته، وذلك، اعتماداً على مستوى الخصوصية الذي تم تحديده. على سبيل المثال، بعد الدخول إلى فيسبوك، يستطيع الشخص أن يدخل إلى أحد الأسماء المعروفة

والذي ربما يكون مُسَجَلًا في فيسبوك - أو إلى اسم أي شخص آخر لنفس الغرض - والنظر إلى الملف الشخصي الخاص بهذا الشخص، وإلى آخر المنشورات المرسلّة من الآخرين، كما يستطيع الوصول إلى أصدقاء ذلك الشخص على الفيسبوك، وحتى الاطلاع على منشوراتهم أيضاً. وسنتحدث بشكل أكبر عن المخاوف المتعلقة بخصوصية الأعمال في هذا المجال في قسم لاحق، ولكن إذا لم يقم مستخدم فيسبوك بتحديد النشاط الذي يقوم به على فيسبوك على أنه نشاط خاص، فإنه يمكن لأحدهم أن يصل في بعض الأحيان إلى معلومات تفوق الحد الذي يريده ذلك المستخدم. على سبيل المثال، قد يرى الشخص بعض الرسائل من نوع "شكراً لدعوتي لل. . . " التي تم إرسالها إلى أحد الأشخاص، وأحياناً مع صورة، وكذلك القدرة على الذهاب إلى صفحة فيسبوك للمرسل. هذه الرسائل المرسلّة تبقى لفترة طويلة، ما لم يتم اتخاذ خطوات مدروسة لحذف السجلات. وعلى الرغم من روعة كل هذا الأمر بالنسبة لحياة الطالب الجامعي، فإن المنشورات والأنشطة المسجلة قد تكون مصدراً لبعض المخاوف المتعلقة بالخصوصية وحتى المخاوف الأمنية في بيئة الأعمال.

ومن الممكن أيضاً أن يكون تطبيق فيسبوك مفيداً في بيئات العمل إذا ما استخدم وسيلة لبناء وإدارة فرق القوة العاملة. فعلى سبيل المثال، بالنسبة للمشاريع التنفيذية للنظم الكبيرة - على غرار الجهود الوارد وصفها في الفصل السادس عشر من هذا الكتاب حول إدارة المشاريع والبرامج - فإن مدير المشروع يمكن أن يطلب من جميع أعضاء فريق المشروع أن يقوموا بإنشاء أو تحديث ملفات التعريف الخاصة بهم على فيسبوك ليتم تثبيتهم بوصفهم أعضاء في فريق المشروع. عندها سيكون من السهل القيام بجدولة وإرسال أحداث المشروع، كما يمكن للمدير المسئول التعرف على المعلومات الأساسية لأعضاء الفريق والدخول إلى ملفاتهم الشخصية بطريقة أكثر لطفاً، على عكس ما يحدث عند قيامه بالوصول إلى سجلات الموارد البشرية التقليدية.

إن حديثنا هنا يُبرز فقط القليل من سمات فيسبوك الآخذة في التوسع. يمكن للمرء الاشتراك لتحميل منشورات من مواقع ويب محددة، ونشر الرسائل أو التواصل من خلال الهاتف الذكي واستقبال رسالة عيد الميلاد التي يمكن نشرها لجميع أصدقاء هذا الشخص على فيسبوك. بالنسبة للمؤسسة التجارية، يتسبب تطبيق الفيسبوك في إثارة بعض المخاطر.

على سبيل المثال، من الممكن أن يقوم أحد الموظفين بإرسال شكوى في منشور على فيسبوك تتعلق بجودة بعض منتجات الشركة أو حتى كفاءة أحد المديرين. فالرسالة التي أرسلت إلى أحد الأصدقاء على فيسبوك على أنها رسالة شخصية يمكن أن يرسلها هذا الصديق إلى أصدقاء الأصدقاء مكونين بذلك شبكة اتصالات واسعة النطاق والتي يكون لها أحياناً مردود على المؤسسة وبعض القضايا الخاصة المتعلقة بها. كما سنتحدث في القسم التالي عن القضايا القانونية الخاصة بوسائل التواصل الاجتماعي، حيث يوجد العديد هنا من قضايا حوكمة تقنية المعلومات.

على الرغم من امتلاك تطبيق الفيسبوك أداة خاصة لبناء صفحات أعمال المؤسسة، والتي تعد إحدى الأدوات القوية لتسويق جميع جوانب العمليات التجارية للمؤسسة، وأن هناك تصاعداً مستمراً في استخدام الفيسبوك باعتبارها إحدى أدوات الاتصال في مجال الأعمال، فإنه يستخدم عادة في هذه الأيام لغايات الاتصالات الشخصية وليس للأعمال التجارية. فإ إنشاء صفحة أعمال على الفيسبوك تعد من الوسائل الجيدة للترويج، وذلك لأن صفحات الأعمال على فيسبوك يمكن مشاهدتها من قبل الملايين من مستخدمي فيسبوك. تعد صفحات فيسبوك تلك بمثابة منصة إعلانية فعالة تقدم أساليب مبتكرة للتسويق عبر الويب، الأمر الذي يسمح بالتفاعل بين أصحاب الأعمال والعلماء. في الحقيقة فإن هذه الصفحات تذهب إلى ما هو أبعد من قضايا حوكمة تقنية المعلومات المذكورة في هذا الفصل، كما أنها تمثل تطبيقاً مؤسسياً قوياً وفعالاً.

لينكدإن LinkedIn:

لينكدإن هو أحد تطبيقات وسائل التواصل الاجتماعي التي تحظى بشعبية كبيرة، ويقوم هذا التطبيق على الشبكات الاجتماعية أو المهنية المرتبطة بالأعمال التجارية، ويستخدم لإجراء اتصالات شبكية بين العديد من المجموعات المهنية، كأعضاء AICPA أو خريجي الجامعات. يعد موقع لينكدإن أيضاً بمثابة منصة اتصالات شعبية بالنسبة للعديد من الفئات المهنية، كمديري المشاريع والمهندسين المدنيين، والجيولوجيين، والمدققين، وغيرهم الكثير. وتعمل تلك المنصة في جميع أنحاء العالم وبعده لغات. وقد كان هناك أكثر من ١٢٥ مليون مستخدم مسجلين في لينكدإن حتى وقت نشرنا لهذا الكتاب.

كانت المرة الأولى التي تعرّف فيها معظم المهنيين على تطبيق لينكدإن من خلال استقبال رسالة بريد إلكتروني من أحد المشاركين المهنيين مصحوبة بدعوة للانضمام إلى إحدى المجموعات الموجودة في لينكدإن، أو للقيام بتأسيس اتصال لينكدإن لبعض المصالح أو الاهتمامات المهنية المشتركة. إذا كان الشخص المدعو جديداً على تطبيق لينكدإن، فإنه يطلب منه التسجيل عن طريق إرسال بعض المعلومات الشخصية، والتي تتعلق غالباً بسيرته المهنية. الأمر الذي يأخذ طابعاً أكثر رسمية مما هو عليه في تطبيق الفيسبوك، الذي من خلاله يطلب من الشخص أن يصبح أحد أصدقاء فيسبوك لشخص ما دون الحاجة إلى إدخال أي معلومات أو تقديم طلب ما.

عند التسجيل في لينكدإن عضواً في إحدى المجموعات المهنية، فإنه يُطلب من المستخدم أن يقوم بتوفير معلومات عن سيرته المهنية وأصحاب العمل الحاليين والسابقين، وكذلك تواريخ تلك الوظائف وغيرها من المعلومات المهنية الشخصية. كما يوجد هناك حيز لنشر سيرة ذاتية كاملة وإعلانات وغيرها من المواد. ويضم النظام أيضاً عملية تسمح للمسجل الجديد أن يطلب جهات الاتصال الخاصة بأرباب العمل والمهنيين السابقين لتقديمها كمراجع. يسمح تطبيق لينكدإن للمستخدمين المسجلين بالاحتفاظ بقائمة تفصيلية بجهات الاتصال مع الأشخاص الذين لديه معهم مستوى معين من العلاقة تسمى زملاء Connections. يمكن للمستخدمين أن يقوموا بدعوة أي شخص (سواء كان مستخدماً للموقع أم لا) ليصبح زميلاً Connection ضمن مجموعة الزملاء، إلا أن المتلقي للدعوة يستطيع اختيار "لا أعرف" ليقوم برفض الدعوة الموجهة إليه. يمكن استخدام زملاء لينكدإن بإحدى الطرق التالية:

- يمكن بناء شبكة اتصال مكونة من الزملاء المباشرين لشخص ما، ويوصف الزملاء الأوائل بزملاء الدرجة الثانية، وأيضاً يوصف زملاء الدرجة الثانية بأنهم زملاء الدرجة الثالثة. يمكن أن يستخدم هذا للحصول على تعريف لشخص ما يرغب في معرفته من خلال الاتصال المتبادل.
- ويمكن بعد ذلك أن يستخدم لينكدإن في العثور على وظائف، وأشخاص، وفرص الأعمال التي أوصى بها شخص ما في شبكة اتصال أحدهم.
- يمكن لأصحاب العمل إدراج الوظائف والبحث عن المرشحين المحتملين.

- يمكن للباحثين عن وظيفة مراجعة الملف الشخصي لمديري التوظيف واكتشاف أي من جهات الاتصال الموجودة يمكن التواصل معهم من خلالها.
- يمكن للمستخدمين نشر الصور الخاصة بهم وعرض صور غيرهم للمساعدة في تحديد الهوية.
- يمكن للمستخدمين متابعة مختلف الشركات والحصول على إشعارات حول المنتجات الجديدة أو غيرها من المعلومات.
- تتطلب آلية الوصول المستخدمة في بوابة تطبيق لينكدإن جهات اتصال لمجموعة من المهنيين المرتبطين بعلاقة سابقة، أو بإدخال إحدى جهات الاتصال الخاصة بهم بنية بناء الثقة بين مستخدمي الخدمة.

ضمن حدود المجالات المتنوعة للموضوعات المتخصصة الموجودة في تطبيق لينكدإن، فإن مواقع هذا التطبيق تعد منتديات نقاشية نشطة تغطي العديد من المجالات المتخصصة في لينكدإن. على سبيل المثال، يتضمن موقع لينكدإن الخاص بالجمعية الوطنية لأجهزة التحكم في الشركات^(٣) سلسلة من النقاشات النشطة. ويجوز لعضو لينكدإن المشترك في هذه المجموعة أن يقوم بطرح سؤال مثل: "كيف يجب على مجلس الإدارة أن يدير مدقيقه الداخليين بشكل أفضل؟" وقد يقوم الأعضاء الآخرون في هذه المجموعة بالرد على هذا السؤال، وقد تكون النتيجة نشوب نقاش ساخن يستمر بين جميع الأطراف.

ولعل الأمر الأكثر أهمية في سمات الاتصالات المهنية الخاصة بتطبيق لينكدإن، هو أنه يشمل سلسلة من التطبيقات المتخصصة التي تهدف للحصول على إرشادات وظيفية وتحليل سير الأعمال، وتعزيز مبيعات المنتجات، وتعزيز الوعي بالعلامة التجارية، والتعامل مع مبيعات التذاكر، والتواصل مع المستثمرين وما هو أكثر من ذلك بكثير. إن تطبيق استطلاعات الرأي الخاص بتطبيق لينكدإن يعد من الأمثلة الجيدة على ذلك. فهو يتيح لمستخدمي لينكدإن إمكانية العثور بسهولة على إجابات لأسئلة تخص أبحاث الأعمال والسوق. فهو يسمح للمؤسسة بأن تقوم بطرح بعض الأسئلة، التي سيقوم تطبيق لينكدإن بتوزيعها على زملائك وعلى الملايين من المهنيين المتواجدين على الموقع. ومن الممكن أيضاً أن يتم مشاركة نتائج الاستطلاعات مع مستخدمي فيسبوك أو تويتر على الحساب

الخاص بالمؤسسة، أو القيام بإضافتها إلى موقع الويب الخاص بالمؤسسة. وهو يعمل تماماً مثل أي خدمة استطلاع أخرى: يمكن لمستخدمي لينكدإن أن يقوموا بطرح سؤال، وإضافة حتى خمسة ردود أو إجابات محتملة، واختيار مدة التشغيل. وبمجرد أن يتم استلام الإجابات ضمن المدة الزمنية المحددة، فإن لينكدإن سيقوم بمشاركة الإجابات مع الشبكات الاجتماعية التي تم تأسيسها أو المواقع الإلكترونية للمؤسسة. نظراً لوجود هذا الرابط القوي في تطبيق لينكدإن، فإن ردود الاستطلاع يمكن تقسيمها للتصويت حسب العمر أو الجنس أو الأقدمية، وهو ما يسمح للإدارة بتحليل أسئلة مثل "هل إجابة الشخص الذي عمره ٢٥ سنة تختلف عن إجابة الشخص الذي عمره ٤٥ سنة؟" أو "هل تختلف إجابات الرجال عن إجابات النساء؟".

إن لينكدإن أكثر من مجرد تطبيق خاص بالأعمال التجارية، كما أنه لا يمتلك البيئة المفتوحة نفسها والمعرضة للمخاطر المحتملة التي يمكن أن نجدها في فيسبوك، فالرسائل المرسلة لأصدقاء فيسبوك يمكن بسهولة تعميمها وإعادة تعميمها على الآخرين. ومع ذلك، ونظراً لأن تطبيق لينكدإن يعتبر وسيلة للاتصالات والنقاش المهني بين مختلف الفئات المهنية المتخصصة، فمن الممكن للبيانات السرية للمؤسسة أن تتسرب بسهولة من خلال مواقع النقاش الخاصة بتطبيق لينكدإن. أحد مهندسي تطوير المنتجات، على سبيل المثال، قد يقوم بالاشتراك في موقع لينكدإن الخاص بمهندسي تطوير المنتج في المؤسسة. كجزء من المناقشات الجارية على الإنترنت عبر تطبيق لينكدإن، قد يقوم مهندس التطوير بالرد بشكل غير سليم على مناقشة عبر الإنترنت عن طريق إعطاء بعض المعلومات السرية للمؤسسة حول نقطة فنية دون أن يدرك طبيعة البيانات الصادرة عنه. أضف إلى ذلك، أن السيرة الذاتية لهذا المهندس قد تكون مفتوحة لشركات التوظيف الخارجي، ويكون هناك استنزاف محتمل لموارد الشركة.

تويتر Twitter:

كانت المرة الأولى التي سمع فيها العديد في الولايات المتحدة الأمريكية عن تطبيق تويتر Twitter في عام ٢٠١١، وذلك عندما حاول عضو الكونجرس الأمريكي، أنتوني وينر Anthony Weiner إرسال صورة خلية له على تويتر إلى مساعدته في الحملة الانتخابية، إلا أن الصورة

قد أرسلت بالخطأ إلى قائمة التوزيع الموجودة في حسابه على تويتر (أو ما يُطلق عليهم المتابعون followers بلغة تويتر)^(٤). وسرعان ما نشرت الصحافة أن عضو الكونجرس آنذاك كان يرسل العديد من الرسائل المشينة الأخرى على حساب تويتر. أجبرت هذه الأحداث وينر على الاستقالة، ومن المؤكد أن حماقته قد تسببت في جعل العديد يسمع عن القدرة الهائلة لتويتر.

تويتر هو خدمة مجانية تسمح لأي شخص أن يقول تقريباً أي شيء لأي شخص آخر ما دامت رسالته لم تتجاوز ١٤٠ حرفاً، فهو نظامٌ يخاطب مستخدمه "ما الذي تقوم به الآن" ويتخلل ذلك تواصل اجتماعي على الإنترنت. واستناداً إلى شعاره الذي يمثله الطائر الأزرق، فإن تويتر يمكن مستخدميه من إرسال وقراءة تلك المنشورات التي تعتمد على النص أو الرسائل القصيرة، المعروفه بشكل غير رسمي باسم "تغريدات Tweets"، والتي تُرسل في كثير من الأحيان من خلال الهاتف المحمول، إما عن طريق الرسائل النصية أو التطبيقات التي تم إصدارها لبعض الهواتف الذكية. وبوجود كل هذه التطبيقات الخاصة بالرسائل، فإن تويتر يعد واحداً من المواقع العشر الأولى الأكثر زيارة في جميع أنحاء العالم. ويشير الاستطلاع الذي أجرته شركة كومبيت دوت كوم Compete.com في شهر فبراير ٢٠٠٩، إلى أن تويتر يشكل الشبكة الاجتماعية الثالثة الأكثر استخداماً، وذلك استناداً إلى إحصائياتهم التي تدل على وجود ستة ملايين زائر جديد في الشهر وخمسة وخمسين مليون زيارة تتم على تويتر شهرياً. وللمساعدة في شرح المصطلحات والمفاهيم الخاصة بتويتر، فإن الشكل التوضيحي (٢-٢١) يسرد البعض منها. وقد يلاحظ العديد من كبار المديرين استخدام موظفيهم لهذه المصطلحات أثناء قيامهم بإرسال تغريداتهم للآخرين.

شكل توضيحي (٢-٢١)

المصطلحات والمفاهيم الخاصة بتطبيق تويتر

- **تغريدة Tweet:** عندما تنشر أو تكتب ١٤٠ حرفاً على تويتر وتنقر إرسال فهي تعد تغريدة أو تويتينغ tweeting.
- **تسجيل حساب Handle:** عبارة عن اسم المستخدم على تويتر في شكل @ducttape. اسم شخصي قصير مشابهة لـ URL.
- **متابعة Follow:** هذا هو الإجراء الخاص بإضافة شخص ما إلى قائمة الأشخاص الذين تتابعهم، مما يجعل تغريداتهم تظهر على الصفحة الرئيسية الخاصة بك.
- **الردود Replies:** وهذا يحدث عندما يكتب شخص ما تغريدة مباشرة على حساب المستخدم - @ducttape أي ثرثرة في منشور هادئ - وأيضاً في كثير من الأحيان يكون دعوة للتواصل مع متابع آخر.
- **إعادة التغريد Retweet:** يعد هذا أسلوباً لإعادة نشر تغريدة شخص آخر، وتبقى التغريدة الأصلية بجانب حساب المؤلف سليمة دون تغيير، ولكنك في الأساس تظهر تغريدة شخص ما إلى الأتباع، والعديد يستخدم هذا لإضافة محتوى ومعرفة المواد من الأشخاص الذين يتبعونه.
- **الرسالة المباشرة DM:** هذا المصطلح عبارة عن رسالة يتم إرسالها مباشرة إلى مستخدم آخر. يجب أن يكون هذا الشخص متابعاً لك لتتمكن من إرسال رسالة مباشرة له أو لها. وهذه تعد أداة مفيدة جداً للرسائل الخاصة.
- **الوسم (هاشتاج) Hashtag:** وهي طريقة يستخدمها الأشخاص لتصنيف التغريدات على سبيل المثال قد يستخدم الآخرون العلامة نفسها، ومن ثم تكون وسيلة فعالة للناس لعرض تغريدات ذات الصلة.

على الرغم من القدرات الهائلة لتويتر على متابعة وحمل سيل كبير من الرسائل المتعلقة بمجموعة كبيرة من الأشخاص والموضوعات، فإن مستخدم تويتر وأحياناً الموظف قد يقضي الكثير من الوقت في قراءة وإرسال هذه التغريدات. على سبيل المثال، قامت شركة بير أناليتكس (Pear Analytics) المعنية باستطلاع أوضاع السوق التي يقع مقرها في سان أنطونيو بولاية تكساس الأمريكية، بتحليل ٢٠٠٠ تغريدة (منشؤها الولايات المتحدة وباللغة الإنجليزية) على مدى أسبوعين في أغسطس ٢٠٠٩ وتم تصنيف الرسائل إلى الفئات الست التالية^(٥):

١- ثرثرة عديمة الجدوى - ٤٠ في المئة

٢- محادثة - ٣٨ في المئة

٣- قيمة تهرير الرسائل - ٩ في المئة

٤- الترويج الذاتي - ٦ في المئة

٥- الرسائل غير المرغوب فيها - ٤ في المئة

٦- أخبار - ٤ في المئة

تشير هذه النتائج إلى أن تويتر يحتوي غالباً على الكثير من "الثروة العديمة الجدوى"، وهو البند الأول في القائمة أعلاه. ولعل الميزة هنا هي أن هذه الرسائل تسمح للمغردين عبر تويتر أن يعرفوا الناس من حولهم فيم يفكرون وماذا يفعلون وبم يشعرون؟ في جميع الأحوال، فإن العديد من هذه التغريدات يشبه إلى حد ما جلسات الحوار التي كانت تتم بين موظفي الشركة أثناء تجمعهم بالقرب من مبرد الماء^(*) في الماضي. كان المدير المخضرم في ذلك الوقت يرفض أو يحد من مثل هذه النشاطات الخاصة بالدردشة حول مبرد المياه. لذا لا بد من عمل محاولات مشابهة للحد من استخدام الموظفين لوسائل التواصل الاجتماعي أثناء العمل.

سواء نظرنا إلى مثال عضو الكونجرس السابق الفاسد وينر Weiner، الذي سبق الحديث عنه، أو إلى أي من الأمثلة الحالية العديدة الأخرى، فإن تويتر يعد أداة قوية يمكن أن تشكل مخاطر على المؤسسة إذا ما تم استخدامها بشكل غير لائق. فكما تحدثنا للتو عن أهمية مدونة قواعد السلوك المهني للمؤسسة في الفصل العشرين من هذا الكتاب، والحاجة إلى إقرار بأن جميع أصحاب المصلحة المعنيين بها قد قاموا بقراءة وفهم المدونة ووافقوا على الالتزام بها، فإنه يجب على المؤسسة أن تطلق سياسة مماثلة لتطبيقات وسائل التواصل الاجتماعي مثل تويتر.

الشكل التوضيحي (٢١-٣) عبارة عن مثال لسياسة المؤسسة المتعلقة باستخدام الموظف لتويتر، وذلك باستخدام العينة الخاصة بنا للشركة العالمية لمنتجات الحاسب. ويمكن تنفيذ سياسات مماثلة لفيسبوك وغيرها من تطبيقات وسائط التواصل الاجتماعي، أو يمكن صياغة السياسة بطريقة تتضمن تطبيقات وسائل التواصل الاجتماعي في المؤسسة، ويتجلى جوهر ذلك في أن مثل هذه السياسات يجب أن تُطلق بطريقة تجعل من جميع الموظفين وأصحاب المصلحة الآخرين يكونون على فهم للمقاصد والمخاطر المحتملة من أي من هذه التطبيقات الخاصة بوسائل التواصل الاجتماعي.

(*) تعني الدردشة العارضة بين مجموعة من عمال الشركة الذين لا يكونون على اتصال مباشر أثناء العمل ويلتقون في استراحة قصيرة عند مبرد الماء للشرب ويمكن تسميتها في هذه الأيام بـ "دردشة التدخين". (المترجم).

شكل توضيحي (٢١-٣)

عينة لسياسة الاستخدام الخاصة بتويتر

الغرض: تصف هذه الوثيقة استخدام حسابات تويتر الشخصية خلال يوم العمل للموظف. وهي لا تنطبق على حسابات تويتر الخاصة بالشركة.

نظرة عامة: تدرك الشركة أن الشبكات الاجتماعية وأدوات التواصل الاجتماعي الخاصة بالموظف تقدم قيمة ما للشركة. ونتيجة لذلك، فقد وضعنا سياسة تسمح بمساحة صغيرة من استخدام تويتر أثناء العمل طالما تم العمل ببعض المبادئ التوجيهية. إذا اعتبرت المبادئ التوجيهية الواردة في هذه السياسة غير مقبولة، فإنه من ثم يُعتبر استخدام الموظف لتويتر أثناء العمل أيضاً غير مقبول.

تقدم هذه الوثيقة مجموعتين من المبادئ التوجيهية. المجموعة الأولى هي التي تنطبق على كل استخدام لتويتر يخص الأنشطة المتعلقة بالشركة، سواء في أوقات العمل أم في الأوقات الشخصية. المجموعة الثانية هي التي تنطبق على أولئك الذين يرغبون في استخدام تويتر أثناء العمل واستخدام حساباتهم للمساعدة في الترويج للشركة.

المبادئ التوجيهية لاستخدام تويتر في الشركة العالمية لمنتجات الحاسب:

١. عدم الإفصاح عن المعلومات السرية أو الخاصة على حساب تويتر الخاص بك. الإفصاح عن المعلومات التنافسية أو الأسرار التجارية يكون سبباً كافياً لإنهاء الخدمة.
٢. تحمل مسؤولية ما تكتب. تذكر أن "إمكانية" أن تقول شيئاً ما لا تعني "إجبارك" على أن تقوله. الكلمات المكتوبة تكون أكثر صعوبة في التفسير من التفاعل اللفظي. تذكر أن ما تقوله سوف يكون بسجل دائم. كن حذراً. كن ذكياً.
٣. كن صادقاً واستخدم الإفصاح الكامل. إذا كنت تتحدث عن أحد منتجات الشركة أو منتج يملكه الطرف المنافس، فمن مصلحتك أن تفصح أنك تعمل لصالح الشركة.
٤. احترم حقوق التأليف والنشر. لا ترسل النص أو الصور أو الفيديو الذي تم إنشاؤه من قبل شخص آخر دون الإسناد الصحيح. إذا كان لديك أسئلة حول قانون حقوق التأليف و/ أو استخدام بعض وسائل الإعلام، اتصل بالقسم القانوني.
٥. تويتر ليست بديلاً للاتصالات داخل الشركة. فيجب أن تنتقل المعلومات الهامة من خلال قنوات الاتصال الطبيعية للشركة، وليس من خلال تويتر.
٦. تويتر ليس بديلاً لخدمة العملاء. رجاء قم بتوجيه العملاء إلى قسم خدمة العملاء بدلاً من التعامل مع الاستفسارات بشكل كلي من خلال تويتر.
٧. كن واضحاً أنك لست الناطق الرسمي للشركة وأن وجهات نظرك لا تعكس بالضرورة وجهة نظر الشركة.

المبادئ التوجيهية لاستخدام تويتر في العمل:	
١. الأمر يقتضي منك القيام بتقديم إما (أ) رابط لموقع الشركة أو (ب) شعار الشركة على صفحة تويتر الخاصة بك.	
٢. أنت مطالب بأن تقوم بتنفيذ إحدى معاملات الشركة على حسابها الخاص على تويتر على الأقل مرة في الأسبوع.	
٣. يجب أن يكون جزء من تغريداتك ذا صلة بالشركة و/ أو المجال الذي تعمل فيه. لا يوجد أي شرط يخص نسبة محددة يجب الوفاء بها من التغريدات، ولكن يعتبر ٢٠٪ من إجمالي التغريدات مستوى مثالياً.	
٤. تذكر ضرورة أن تكون منتجاً، ذلك أن تويتر يمكن أن يبتلع وقتك ويمكن أن يمنعك من إكمال المهام الأخرى المتعلقة بالعمل. فاستخدم حكمتك لضمان أن يكون لديك متسع من الوقت لاستكمال جميع الأعمال العادية الخاصة بك.	
لقد قرأت هذه السياسة الخاصة بالشركة العالمية لمنتجات الحاسب فيما يخص استخدامي لتويتر، وأنا أفهم إرشادات هذه السياسة، وأوافق على الالتزام بالقواعد والإرشادات الموضحة في هذه السياسة.	
الاسم:	رقم الموظف:
التوقيع:	التاريخ:

نقاط ضعف حوسبة وسائل التواصل الاجتماعي في المؤسسة ومخاطرها:

من الممكن أن يكون التساؤل المنطقي الذي يدور بداخل أحد المسؤولين التنفيذيين هو، "أنا أحد كبار المديرين في المؤسسة. لماذا يجب علي أن أقلق جراء استخدام الموظفين وغيرهم من أصحاب المصالح لفيسبوك، وتويتر، وغيرها من أدوات التواصل الاجتماعي في بيئة العمل ماداموا ينجزون المهام الخاصة بهم؟" هذا النوع من الأسئلة الذي يطرحه العديد من كبار المديرين عندما لا يدركون في الواقع طبيعة هذه التطبيقات التي تبدو في الظاهر أنها تطبيقات شخصية واجتماعية.

وكثيراً ما تبدو المواقع الخاصة بوسائل التواصل الاجتماعي أنها اجتماعية وخارج إطار الرقابة الخاص بمعظم نظم الأعمال وعملياتها واهتماماتها. وكثيراً ما ينظر إليها وكأنها فقط عبارة عن وسيلة تسلية للموظفين، مثل الجهود المشتركة التي تقوم بها لجنة التخطيط لإقامة حفلة الإجازة السنوية. ومع ذلك، فإنه يمكن للقضايا أو المسائل المتعلقة بوسائل

التواصل الاجتماعي أن تذهب إلى ما هو أبعد من مجرد أن تكون عبارة عن رسائل اجتماعية ودية، كاحتمالية أن يرى أشخاص آخرون هذه الرسائل وأن يبادروا باتخاذ إجراءات معينة تستند إلى هذه الرسائل والمعلومات المتبادلة.

لقد أبرزت المقالة الأخيرة في صحيفة شيكاغو تريبيون Chicago Tribune كيف أن دردشة الموظف على فيسبوك يمكن أن تتسبب في مشاكل للمؤسسة. فقد تحدث الموظفون لدى تاجر سيارات باستخفاف فيما بينهم على الفيسبوك عن الطريقة التي يمكن أن يستخدمها صاحب العمل لكي يتجاهل قوانين العمل في الولايات المتحدة^(١). وقد تم تمرير الرسائل التي كان من المفترض أن تكون خاصة بهم في نهاية المطاف إلى سلطات قانون العمل في الولايات المتحدة، الأمر الذي أدى إلى اتخاذ الإجراءات القانونية ضد صاحب العمل. إن الرسائل المرسلة من خلال نظم وسائل التواصل الاجتماعي تحمل بعض المخاطر! يُنظر أحياناً إلى نظم التواصل الاجتماعي على أنها إحدى الموارد الخاصة بالموارد البشرية، وأنها إحدى النشرات غير الرسمية للشركة. ومع ذلك، فإن المؤسسة تواجه العديد من المخاطر المتعلقة بنظم وسائل التواصل الاجتماعي، والتي قد تتضمن فقدان السمعة وخسارة المكانة المرموقة والتعرض للمساءلة القانونية، وذلك عندما يقوم الموظفون بإفشاء الأسرار ونشر الصور والفيديوهات المتعلقة بالأمور التي يجب أن لا يفعلوها. هناك أيضاً مخاطر أمنية على الحاسبات الآلية من البرمجيات الخبيثة، وسرقة الهوية، وذلك من خلال ما يسمى التصيد الاحتيالي phishing، وخرق خصوصية البيانات الحساسة التي تم الحديث عنها في الفصل العاشر من هذا الكتاب.

إن المسؤولية عن المخاطر المرتبطة باستخدام الموظف لتطبيقات مثل فيسبوك وتويتر وغيرها من وسائل التواصل الاجتماعي تتجاوز حدود إدارة أمن تقنية المعلومات، حيث إن المسؤولية الأساسية تقع على عاتق إدارة المؤسسة. حيث يتم تشغيل هذه التطبيقات بشكل عام عبر الإنترنت والنظم الخارجية الخاضعة لسيطرة الشركة.

ترتبط العديد من مخاطر تقنية المعلومات المتعلقة بوسائل التواصل الاجتماعي والمخاوف الإدارية بالسلوك الفردي الذي يحدث خارج حدود البنية التحتية للمؤسسة ونظم تقنية المعلومات الخاصة بها. في جميع الحالات، فإن نظم وسائل التواصل الاجتماعي

تحمل في طياتها قضايا تتعلق بالمحتوى وحرية التعبير. وترتبط هذه الممارسات الخاصة بوسائل التواصل الاجتماعي بشكل وثيق بالعديد من القضايا التي وردت في الفصل العشرين من هذا الكتاب الذي تحدث عن الحاجة إلى وجود ثقافة أخلاقية في أماكن العمل. وهو الفصل الذي تحدث أيضاً عن أهمية الرسائل والسياسات القوية للإدارة مثل مدونات قواعد السلوك وبيانات المهمة أو الرسالة التي تساعد المؤسسة وأصحاب المصالح فيها على التفكير بطريقة صحيحة وإيجابية. في جميع الأحوال، يجب على المؤسسة أن تكون على علم ببعض المخاطر والمخاوف المتعلقة بوسائل التواصل الاجتماعي التالية:

- **القضايا المتعلقة بإنتاجية الموظف:** ربما تميل هذه القضايا بشكل أكبر نحو الجانب الإداري من حيث تحديد أهداف الموظفين ومسئولياتهم، وإن كان الموظفون على مختلف مستوياتهم يقومون أحياناً بقضاء وقت طويل في إرسال الملاحظات والصور لأصدقائهم، سواء كانوا من داخل الشركة أم خارجها، وسواء عبر تويتر أم عبر فيسبوك أو بعض تطبيقات وسائل التواصل الاجتماعي الأخرى. ففي بعض النواحي، قد لا يختلف هذا كثيراً عن الأشخاص الذين يقضون أوقاتاً طويلة على المكالمات الهاتفية الشخصية، إلا أنه من الصعب القيام بمراقبة وكشف هذا النوع من الأنشطة الخاص بوسائل التواصل الاجتماعي.
- **نقص الرقابة المفروضة على المحتوى المؤسسي:** قد يقوم الموظفون وأصحاب المصلحة بشكل مقصود أو غير مقصود بنشر معلومات خاطئة أو غير لائقة على مواقع وسائل التواصل الاجتماعي. هذا النوع من المعلومات يمكن أن ينقل إلى العديد من الأشخاص الآخرين من خلال الطبيعة التتابعية للعديد من أدوات وسائل التواصل الاجتماعي. فبمجرد أن تبدأ المعلومات المغلوطة في النشر، فإنه يكون من الصعب إيقافها.
- **عدم الامتثال للوائح التنظيمية الخاصة بإدارة السجلات:** على الرغم من حقوق التأليف والنشر وقواعد حماية البيانات، فإنه من السهل جداً بالنسبة لأصحاب المصلحة أن يقوموا بنسخ وإرسال الوثائق المحمية عبر أنظمة وسائل التواصل الاجتماعي. وفي حال تم إرسال هذه السجلات بشكل غير صحيح أو غير قانوني فإن المؤسسة ستعرض للمخاطر.
- **الفيروسات وبرامج التجسس:** يوجد هناك العديد من الحوادث المسجلة التي تم فيها استخدام وسائل التواصل الاجتماعي أو مواقع الشبكات ذات الصلة لنشر البرمجيات

الخبیثة كالفیروسات^(٧)، ومن المؤكد أن نظم التواصل الاجتماعي ليست الوسيلة الوحيدة المستخدمة في هذا الصدد. ومع ذلك، فإن مواقع الشبكات الاجتماعية على أرض الواقع ربما لا تشكل تهديداً أكثر من الذي يشكله أي نوع آخر من مواقع شبكة الإنترنت.

• **مشاكل عرض النطاق الترددي:** كانت مسألة عرض النطاق الترددي للبيانات Bandwidth تفوق بكثير أي مسألة أخرى في الأيام الأولى لظهور الاتصالات والإنترنت، فهو مصطلح يشير إلى "حجم القناة" أو كمية البيانات المنقولة عبر خطوط الاتصالات. إن إرسال الناس لكميات كبيرة من الصور الرقمية أو غيرها من المواد التي تعتبر إلى حد ما كبيرة الحجم قد تؤدي إلى اختناق النظام. وعلى الرغم من أن هذا الأمر لا يعد معضلة كبيرة بالنسبة لشبكة الإنترنت، فإنه يمكن مثل هذا النوع من المواد الكبيرة الحجم أن تعيق خط الاتصالات لمؤسسة صغيرة ويؤدي إلى انسدادها.

• **القضايا الأمنية للمؤسسة:** هناك العديد من الثغرات في هذا المجال. حيث يمكن أن يستخدم الجاني مثلاً الهاتف الخليوي للقيام بالتقاط صورة لإحدى الوثائق السرية أو المنتجات أو المرافق الموجودة، ويقوم بعد ذلك بكل سهولة ويسر بإرسال هذه المواد التي التقطها إلى شخص أو أكثر بواسطة أداة مثل فيسبوك من خلال بضع ضربات أو ضغطات سريعة على لوحة المفاتيح. ولذلك فإن هناك حاجة إلى ضوابط مادية وبيانات جيدة تخص سياسة التبليغ وبيئة أخلاقية قوية للمؤسسة.

• **قضايا المسؤولية في وسائل التواصل الاجتماعي:** يمكن أن تتحمل المؤسسة المسؤولية عن الرسائل التي تُرسل بواسطة أحد الموظفين خلال الوقت المخصص للعمل في المؤسسة، وذلك بالنسبة للمنشورات التي تتم بواسطة موارد تقنية المعلومات المؤسسية. وعلى الرغم من أن القانون حقيقة لا يزال غير واضح حتى الآن، فإنه وجد أن الأفراد هم المسئولون عن إرسال الرسائل التي تتطلب مزيداً من الحذر إلى مواقع الشبكات الاجتماعية. لذا يجب على المؤسسة ووحدات الأعمال توخي الحذر في مثل هذه الحالات، فهي بالتأكيد تشكل مخاطر يجب أخذها بالحسبان.

ولأن استخدامنا لأدوات التواصل الاجتماعي في ازدياد، فإنه لا يمكننا سوى أن نتوقع استمرار هذا التوجه أو التيار. ولأن معظم أصحاب المصلحة في المؤسسة لديهم أجهزة

هاتف ذكي خاصة، فضلاً عن اتصالات الإنترنت الموجودة في منازلهم، فإن جميع هؤلاء الأشخاص تقريباً يستطيعون الوصول إلى المواقع الخاصة بوسائل التواصل الاجتماعي. البعض من هؤلاء يقوم باستخدام هذه الأدوات بشكل مكثف، ومن الممكن أن تصبح الحدود الفاصلة بين الأنشطة الشخصية والنظم المكتبية ضبابية. وفي حال قامت المؤسسة بفرض سياسة منع استخدام وسائل التواصل الاجتماعي أثناء ساعات العمل، فإنها بذلك تكون وكأنها تنظر إلى الموضوع عبر نظارة وردية. ونحن بشكل عام لا نعمل في المؤسسات فقط من الساعة التاسعة صباحاً إلى الساعة الخامسة مساءً مثلاً، بل نحن منخرطون في الأنشطة الخاصة بالأعمال أثناء وجودنا في المنزل وأثناء سفرنا كذلك. ومن ثم لا يمكننا في مثل هذه الحالة أن نضع حدوداً فاصلة.

كما أن استخدام أدوات التواصل الاجتماعي في أنشطة الأعمال ينمو أيضاً. كما تحدثنا منذ قليل عن أداة الاقتراح الخاصة بتطبيق لينكدإن، والتي يمكن اعتبارها نظاماً شائع الاستخدام في أماكن العمل. وسنرى على نحو متزايد مدى تقارب وترابط الخطوط الفاصلة بين استخدام وسائل التواصل الاجتماعي في الأمور الشخصية أولاً وبين استخدامها في الأنشطة المتعلقة بالأعمال. إن السبيل الوحيد للحد من المخاطر والحصول على فهم أفضل لحوكمة تقنية المعلومات الخاصة باستخدام أدوات التواصل الاجتماعي في أماكن العمل، هو إيجاد سياسات تتعلق بالاستخدام الفعال لهذه الأدوات وتبليغها بصورة جيدة إلى جميع أصحاب المصلحة في مكان العمل داخل المؤسسة.

سياسات وسائل التواصل الاجتماعي:

تحتاج المنشأة إلى وضع ممارسات تثقيفية توضح ما يجب الأخذ به وما يجب تركه من النظم المختلفة لوسائل التواصل الاجتماعي، هذا إلى جانب وضع سياسات محددة خاصة باستخدام أصحاب المصالح لتلك الأدوات. ويجب أن تكون السياسات المتعلقة باستخدام وسائل التواصل الاجتماعي عبارة عن مجموعة فرعية من سياسات الشركة تماماً كمدونات قواعد السلوك، وكذلك سياسات الأمن والخصوصية لتقنية المعلومات التي يتم إيصالها لجميع الموظفين وأصحاب المصلحة. فلننظر على سبيل المثال إلى ما تم الحديث عنه بمزيد من التفصيل في الفصل العشرين من هذا الكتاب، حيث يتعين على المؤسسة وضع سياسة

محددة لوسائل التواصل الاجتماعي لأصحاب المصلحة بشكل عام والتي تحدد سياسات الشركة على مستوى عال جداً بأسلوب سهل فهمه. كما يجب أن يتم تنقيح المدونة وتحديثها بانتظام وينبغي أن يُطلب من جميع أصحاب المصلحة بأن يؤكدوا أنهم قد قاموا بقراءة المدونة وفهموها ووافقوا على الالتزام بها. إن تنفيذ مثل هذه المدونة لقواعد السلوك يعد أمراً هاماً بالنسبة للممارسات القوية والفعالة لحوكمة تقنية المعلومات في المؤسسة. الشكل التوضيحي (٤-٢١) مثال على السياسة العامة لوسائل التواصل الاجتماعي في المؤسسة والتي من شأنها أن تكون مصممة لتتطبق على جميع أصحاب المصلحة الذين يستخدمون تطبيقات وسائل التواصل الاجتماعي في المؤسسة، بدءاً من الموظفين ووصولاً إلى الإدارة العليا، ويمكن تطبيق هذه السياسة على جميع التطبيقات الخاصة بوسائل التواصل الاجتماعي التي قد تؤثر في المؤسسة، سواء كان ذلك من خلال إحدى المبادرات أو التطبيقات المعتمدة على النظام والقائمة على المؤسسة أم من خلال استخدام أحد الأجهزة الشخصية.

شكل توضيحي (٤-٢١)

سياسة وسائل التواصل الاجتماعي في المؤسسة

تُطبق هذه السياسة على جميع أدوات التواصل الاجتماعي، وتستخدم داخل العمل وخارجه، بالنسبة لعمليات تشغيل الأعمال في المؤسسة. بالإضافة إلى الإرشادات الأكثر تحديداً التي تم مناقشتها أدناه، يجب على أي شخص يستخدم أدوات وسائل التواصل الاجتماعي في الأعمال الشخصية أو التجارية ما يلي:

- تعامل مع الآخرين كما تحب أن تُعامل.
- أضف قيمة لعملائك، وصناعتك وعملك.
- اتسم بالاحترام والمهنية واللطف.
- قدم الرؤية، والخبرة، والدراسة ذات الصلة.
- تواصل أخلاقياً ومعنوياً في دعم أهدافك المهنية.

وبالإضافة إلى ذلك، يتعين على جميع أصحاب المصلحة في المؤسسة إبقاء المبادئ التالية في الاعتبار:

فكر قبل أن تنشر:

ضع في الاعتبار أن معظم منصات الحوسبة الاجتماعية على الإنترنت مثل الأسواق العامة، ما يتم عرضه هناك يكون متاحاً ويراها الجميع. على المنصات الاجتماعية، تكون حدود المعلومات المهنية والشخصية دائماً غير واضحة. في هذه الأيام التي تتميز بتحويل سياسات الخصوصية والفهرسة القوية لمحرك البحث، لا يمكنك أن تكون دائماً على يقين مما يتم مشاركته أو ما تم الاطلاع عليه أو ما تمت أرشفته. لاحظ أن ما تنشره على الإنترنت سوف يكون عام لفترة طويلة جداً. ما قمت بنشره سينعكس عليك، لذلك التزم الطريقة التي ترغب في أن تظهر بها أمام الشركة، والأصدقاء، والعائلة، والزملاء، والعملاء. إذا كنت غير متأكد من أن محتوى معيناً مناسب لمشاركته عبر الإنترنت، فلا تنشره. لأن تكون آمناً أفضل لك من الاعتذار.

المسؤولية:

أنت مسؤول شخصياً عن كلماتك وأفعالك، بغض النظر عن مكان وجودك، ما دمت موجوداً على شبكة الإنترنت. رجاء تذكر أنك عندما تشارك في وسائل التواصل الاجتماعي، فإنك تتحدث كفرد وليس نيابة عن الشركة. عرف نفسك دائماً باستخدام صيغة الأفراد لضمير المتكلم.

عندما تناقش معلومات تتعلق بالشركة على شبكة الإنترنت، تحلّ بالشفافية من خلال إعطاء اسمك ودورك واذكر أنك تعمل لصالح الشركة. إذا كان لديك موقع فردي يشير إلى الشركة أو له تأثير فيها، فاستخدام إخلاء المسؤولية مثل "إن الآراء الواردة في هذا الموقع تخصني ولا تخص [اسم الشركة]".

أيضا يسمح به القانون المعمول به فاعلم أن الشركة تحتفظ بالحق في مراقبة استخدام المنصات الاجتماعية واتخاذ الإجراءات المناسبة للحماية ضد إساءة الاستخدام التي يمكن أن تكون ضارة بسمعة الشركة.

أن تقوم بإنشاء حساب للشركة أو أن تصبح الممثل الرسمي الذي يتقاسم المعلومات حول الشركة ومجالات عملنا، يتطلب موافقة من المستوى المناسب من الإدارة. هذه الحسابات فقط قد تعرض شعار الشركة.

السلوك:

يجب أن يكون سلوكك على الإنترنت متفقاً مع مدونة أخلاقيات العمل. لديك فرصة للمساعدة على إظهار سمعة الشركة على الإنترنت. استخدم خبرتك الواسعة لإثراء المناقشات، ساعد في حل المشاكل، وشاركنا الحماس في بيئة عملنا، وشجع التعلم ومشاركة الأفكار. تذكر دائماً أن النعمة التي تستخدمها عبر الإنترنت يمكن أن تُفسر بطرق مختلفة من قبل القراء، نظراً لعدم وجود تواصل شفهي أو اختلافات ثقافية. وقد لا يكون بعض المشاركين على دراية بالاختصارات والوجوه التعبيرية والرموز الشائعة الأخرى المستخدمة في الاتصال عبر الإنترنت. تذكر أيضاً أن التعليقات تُنتزع من سياقها غالباً، لذلك تمسك والتزم بالحقائق. الثقة هي العنصر الرئيسي في بناء علاقات عبر الإنترنت. بناء الثقة عن طريق الحفاظ على لهجة محترمة، حتى عندما تختلف مع الآخرين، ومن خلال ردك على التعليقات في الوقت المناسب أو في حينها. إذا كنت تدرك أنك قد أخطأت، حاول أن تصحح ذلك على الفور. لا تشارك في أي سلوك على الإنترنت من شأنه ألا يكون مقبولاً في مكان عملك أو غير قانوني. على سبيل المثال، لا تدل بتصريحات مهينة أو تستأسد أو ترهب أو تضايق مستخدمين آخرين أو تسبهم أو تنشر محتوى يحض على الكراهية أو القذف أو التهديد، أو التمييز، أو الإباحية.

السرية:

قم دائماً بحماية المعلومات السرية وغيرها من المعلومات المتعلقة بالملكية والخاصة بشركتنا وعملائنا وموردنا. لا تضع أي محتوى على الإنترنت لا ترغب في مشاركته مع صحفي أو عميل أو محلل أو منافس. تأكد من أن أي إشارة إلى معلومات تجارية وعملاء وموردين لا تنتهك أي التزامات عدم إفصاح. رجاء تذكر أيضاً التزامات السرية الخاصة بك بموجب اتفاقية العمل الخاص بك. لا تفصح عن معلومات عن الزملاء أو غيرهم من الأشخاص، أو تسئ استخدام بياناتهم الشخصية، أو تنشر صورهم دون إذن منهم. استخدم دائماً الحكمة في التعامل مع المعلومات التي من الممكن أن تكون حساسة. لا تستخدم منصات الحوسبة الاجتماعية لتبادل المعلومات ذات الطابع السري للشركة أو العملاء أو الموردين، ما لم يتم إيقاف عملية الحصول على مثل هذا النوع من المعلومات وتم إزالة المحتوى من المنصة لمستويات أمنية مناسبة. المواقع العامة ليست المواقع المناسبة للاتصال الداخلي مع موظفي الشركة الآخرين.

حقوق الطبع والنشر:

امتثل للقوانين واللوائح، وعلى الأخص بالقوانين التي تحكم حقوق الملكية الفكرية، متضمناً ذلك حقوق الطبع والنشر والعلامات التجارية. يجب ألا تنشر محتوى أو تتخذ أي إجراء يخالف القانون أو ينتهك حقوق الشركة أو حقوق الملكية الفكرية لأي طرف ثالث.

أفكار أخيرة:

استخدام منصات الحوسبة الاجتماعية وفقاً لهذه السياسة يمكن أن يكون أداة اتصال فعالة وقوية جداً. كونوا فخورين بما تعملون وامتنعوا بالشعور بالإنجاز في البحث عن أفضل جودة وكفاءة أكبر. قبل كل شيء، رجاء استخدم حكمتك وانتبه للآخرين وتحمل عناء الاستماع وإيضاح فكرك بشكل مفهوم.

اعتماداً على مستوى الاستخدام في المؤسسة، فإنه يمكن إطلاق سياسات مماثلة لفيسبوك، وغيرها من وسائل التواصل الاجتماعي. وعلى الرغم من أنه يمكن صياغة سياسة عامة لكافة تطبيقات وسائل التواصل الاجتماعي للمؤسسة، فإنه يفضل عادة وضع بيانات سياسة محددة لكل تطبيق، مثل تويتر وفيسبوك. والفكرة هي إيصال الرسالة لجميع أصحاب المصلحة وهي أن استخدامهم لمختلف تطبيقات وسائل التواصل الاجتماعي في أماكن العمل يحمل بعض المخاطر والفرص بالنسبة للمؤسسة ومساراتهم الوظيفية.

إن تطبيقات وسائل التواصل الاجتماعي تثير بعض القضايا القوية الخاصة بحوكمة تقنية المعلومات في المؤسسات هذه الأيام. وعلى الرغم من أننا ركزنا في هذا الفصل على تطبيقات فيسبوك وتويتر ولينكدإن التي ربما تكون الأكثر استخداماً هذه الأيام، فإن هذا لا يضمن أن تبقى تلك التطبيقات هي الأبرز خلال السنوات القليلة القادمة. وفي جميع الأحوال، تمثل المفاهيم الخاصة بتلك التطبيقات تغييراً تاماً في طريقة تطوير ومعالجة البيانات والتي من شبه المؤكد أنها لن تتغير. على الرغم من أن كبار المديرين قد ينظرون إلى هذه التطبيقات كما لو كانت عبارة عن أدوات لأطفالهم في المنزل أو في المدرسة، أو للموظفين الشباب في الكادر الوظيفي، فإنه يجب على كل واحد من كبار المديرين أن يصبح لديه ولو على الأقل مستوى فهم بسيط بهذه الأدوات من أجل فهم أفضل لهم والتواصل مع الآخرين في المؤسسة.

ملاحظات:

1. Scott Gilbertson, "Feb. 16, 1978: Bulletin Board Goes Electronic," Wired, February 16, 2010, wired.com/thisdayintech/20100216/02/cbbs-first-bbs-bulletin-board/.
٢. يشير مصطلح "ست درجات من الانفصال" إلى فكرة أن كل شخص على وجه الأرض، من خلال طريقة التقديم، يبعد عن الآخر في المتوسط ست خطوات تقريبا، لذلك يمكن عمل سلسلة من بيانات "صديق الصديق" لتوصيل أي شخصين في ست خطوات أو أقل، في المتوسط.
٣. يمكن للمدير التنفيذي الانضمام إلى موقع الجمعية الوطنية لمديري الشركات (NACD) عن طريق تسجيل الدخول إلى لينكدإن ثم النقر للانضمام إلى مجموعة (NACD). سيقوم مدير الموقع بمراجعة بيانات اعتماد الطالب وربما قبولها ومن ثم السماح لهم فيما بعد بالمشاركة في مناقشات الجمعية.
4. "Anthony Weiner Resigns: Timeline of Photos, Twitter Scandal Fallout," Huffington Post, June 16, 2011, www.huffingtonpost.com/2011/06/16/anthony-weiner-resignsscandal_n_878161.html; "Rep. Anthony Weiner Retains Lawyer amid Frenzy over Lewd Twitter Photo," Fox News, May 31, 2011, www.foxnews.com/politics/2011/05/31/rep-weiner-retains-lawyer-amid-frenzy-lewd-photo/.
5. Jennifer Van Grove, "Twitter Analysis: 40% of Tweets Are Pointless Babble," Mashable Social Media, August 12, 2009, <http://mashable.com/2009/12/08/twitter-analysis/>.
6. "Social Media Emerges as Battleground for Protected Speech at Work," Chicago Tribune, September 2, 2011, http://articles.chicagotribune.com/201102-09/business/ct-biz-0902-chicago-law-20110902_1_social-media-labor-laws-employment-law.
٧. سوف يعرض البحث في جوجل العديد من الحوادث المبلغ عنها في هذا الصدد. وللإطلاع على إحدى عينات سجل الحوادث، انظر

"<http://socialsmarty.com/small-business/should-social-networks-be-banned-at-the-workplace/>."

الفصل الثاني والعشرون

حوكمة تقنية المعلومات ودور لجنة تدقيق تقنية المعلومات

تناولت الفصول السابقة العديد من الجوانب والعمليات اللازمة لفهم وتحسين حوكمة تقنية المعلومات في المؤسسة. وقد كان جميع ما تناولناه من تعليقات وتدابير مقترحة خاصة بحوكمة تقنية المعلومات موجهاً إلى جميع مؤسسات الأعمال على اختلاف أنواعها وأحجامها، على الرغم من أننا ركزنا أكثر على الشركات الكبيرة المتعددة الجنسيات والوحدات والتي تتجاوز غالباً الحدود الدولية. إلا أن بعض هذه الممارسات الخاصة بحوكمة تقنية المعلومات قد يكون أيضاً مكلفاً بالنسبة للمؤسسة الصغيرة، في حين أن البعض الآخر يتطلب مساهمات إدارية كبيرة. فعند تنفيذ أي عملية خاصة بحوكمة تقنية المعلومات، ينبغي على الإدارة دائماً النظر في التكاليف المترتبة على ذلك ومن ثم توازن بينها وبين المنافع العائدة.

ويختتم هذا الفصل الأخير بالحديث عن دور لجنة التدقيق التابعة لمجلس الإدارة، الذي يعد أحد العناصر الهامة جداً بالنسبة للشركة ولحوكمة تقنية المعلومات. إننا ننظر غالباً إلى لجنة التدقيق فقط من ناحية الدور الذي تلعبه في مهام الإشراف والتدقيق الداخلي فضلاً عن قيامها بتنسيق أنشطة التدقيق الخارجي. حيث إن لجنة التدقيق هي التي تقوم بتحديد نظام أو أسلوب العمل بالنسبة للعديد من الأنشطة الخاصة بحوكمة تقنية المعلومات. وسيقوم هذا الفصل بعرض الدور الذي تلعبه لجنة التدقيق من أجل وضع نظام أو أسلوب العمل المتبع لمراجعة الأنشطة الخاصة بحوكمة تقنية المعلومات في المؤسسة.

لجنة التدقيق التابعة للمؤسسة وحوكمة تقنية المعلومات:

تدار الشركات العامة من قبل مجالس الإدارة المنتخبين من قبل المساهمين، والمسؤولة عن الأنشطة الرئيسية للإدارة. ومن الممكن أن يكون أعضاء مجلس الإدارة المنتخبين في بعض الأحيان جزءاً من الكادر الإداري، أو أن يكونوا مديرين مستقلين لا تربطهم بالشركة أية علاقات مباشرة. وتعد لجنة التدقيق أحد المكونات الرئيسية في مجلس إدارة الشركة، فهي المسؤولة عن مراقبة الضوابط الداخلية والتقارير المالية. ونظراً لهذه المسؤولية الرقابية

ومتطلبات قانون ساربينز أوكسلي (SOX)، فإنه يجب أن يكون أعضاء لجنة التدقيق مديرين مستقلين لا تربطهم أي علاقة بإدارة المؤسسة. لا يوجد أي قيود مفروضة على حجم اللجنة، إلا أن المجلس المكتمل المكون من ١٢ إلى ١٦ عضواً يمتلك غالباً لجنة تدقيق مكونة من ٥ إلى ٦ أعضاء. ومن الممكن أن تقوم لجنة التدقيق بدعوة أعضاء من الإدارة أو غيرهم لحضور اجتماعات اللجنة وحتى المشاركة في مداولاتها ونقاشاتها. ومع ذلك، لا يمكن للضيوف الخارجيين أن يكونوا أعضاء يتمتعون بحق التصويت بالكامل، وذلك بموجب قواعد قانون ساربينز أوكسلي SOX. إن مجلس إدارة المؤسسة هو الكيان الرسمي الذي يمنح مسؤولية الحوكمة الشاملة لمالكي ومستثمري ومقرضي المؤسسة. وقد يتحمل جميع أعضاء مجلس الإدارة المسؤولية القانونية عن أفعالهم التي يتخذونها حيال أي قضية، ويقوم المجلس ولجانه باعتماد معظم الأعمال الرسمية من خلال إصدار قرارات تصبح بدورها مواد ثابتة في سجل المؤسسة.

وكما هو واضح هنا، قد تكون مجالس إدارات الشركات مكونة مما يعرف بالمديرين الداخليين أو الخارجيين. فالمديرون الداخليون هم الأعضاء المنتظمون في الإدارة والذين يقومون أيضاً بالخدمة في مجلس الإدارة. مثل، الرؤساء التنفيذيين CEOs، والمديرين الماليين CFOs، والذين يلعبون أدواراً مزدوجة من خلال الإدارة التنفيذية لمهام العمل، ثم بعد ذلك الإشراف على العمليات التشغيلية للإدارة نفسها من خلال وجودهم في مجلس الإدارة. وباعتبارهم من كبار المديرين التنفيذيين في المؤسسة، فإنه يتعين عليهم امتلاك معرفة واسعة عن شركتهم، إلا أن تلك المعرفة لا تصب دائماً في مصلحة الخارج، وهم المساهمون والمستثمرون المستقلون. الأمر الذي أدى إلى ظهور انتقادات تصف المديرين الداخليين في بعض الأحيان بأنهم كالثعالب التي تحرس أقفاص الدجاج.

فالمدير الخارجي، أو ما يسمى غالباً بالمدير المستقل، هو الشخص الذي ليس لديه أي ارتباط مباشر بالعمليات التشغيلية اليومية للشركة، ولا يتقاضى أية رواتب أو أجور من الشركة جراء مشاركته في اجتماع مجلس الإدارة. يسافر المديرون المستقلون عادة إلى المدينة لحضور اجتماعات مجلس الإدارة، إذ إنهم لا يملكون مكاتب دائمة في المؤسسة وليسوا جزءاً من الكادر الوظيفي الخاص بها. حيث يُنظر إليهم على أنهم في وضع أفضل

لاتخاذ القرارات مثل إغلاق أحد المكاتب، ولا ينظر إليهم على أنهم يتصرفون لخدمة مصالحهم الشخصية.

في السنوات التي سبقت قانون ساربنز أوكسلي SOx، كان للعديد من الشركات مجالس إدارة مكونة من مسؤولي الشركة والأصدقاء والمقربين من المدير المالي CFO. وكانت المجموعة الأخيرة (المقربون) في بعض الأحيان غير مؤهلة تماماً للعمل في هذه المناصب في مجلس الإدارة، وكانوا يتصرفون بموجب تعليمات المدير المالي. وفي الواقع أصبح الوضع في غاية الصعوبة مع سقوط شركة أنرون وإطلاق قانون ساربنز أوكسلي SOx بين عامي ٢٠٠٢-٢٠٠٣. فقد اكتشفت لجنة الكونجرس الأمريكي التي حققت في كارثة شركة أنرون، من بين العديد من الأمور الأخرى، أن المجلس غير مستقل تماماً، وأنه قد استفاد من "عقود الاستشارات" التي مُنحت له من قبل المدير المالي فضلاً عن وجود نقص واضح في الفهم الشخصي للمعاملات المالية المعقدة الخاصة بشركة أنرون في ذاك الوقت.

لقد فرض القانون التشريعي ساربنز أوكسلي SOx، كما مر معنا في الفصل الثاني من هذا الكتاب، سلسلة من المتطلبات الخاصة بمجلس الإدارة، والتي جاءت بهدف تحسين حوكمة الشركات. كان من بين تلك المتطلبات، أن لجنة التدقيق الآن يجب أن تتكون فقط من المديرين الخارجيين؛ الأمر الذي يمنحها استقلالية تامة عن إدارة الشركة، وأن تكون، أو على الأقل ينبغي، أن تكون مؤلفة من مجموعة مؤهلة ومتخصصة من المديرين الخارجيين القادرين على فهم ومراقبة وتنسيق وتقييم بيئة الضوابط الداخلية والأنشطة المالية المتعلقة بالمجلس بأكمله. ولكي تتمكن لجنة التدقيق من الوفاء بمسؤولياتها تجاه كل من مجلس الإدارة وأصحاب المصالح والجمهور، فإنها بحاجة إلى إنشاء وإدارة وحدة خاصة بالتدقيق الداخلي والتي يجب أن تكون عبارة عن مجموعة مستقلة من الأذان والعيون في المؤسسة، وأن تقوم بتقديم التقييمات المتعلقة بالضوابط الداخلية وغيرها من الأمور الأخرى.

ويعتمد ذلك على بنية أو هيكل الشركة، كالشركات التي تتعامل بالأوراق المالية والمسجلة لدى هيئة الأوراق المالية والبورصة الأمريكية، كما تستطيع الشركات الخاصة الأخرى أيضاً

الاستفادة من هذه البنية الخاصة بلجنة التدقيق. على سبيل المثال، هناك العديد من المؤسسات غير الربحية أو الخاصة التي تكون كبيرة بما يكفي لتمتلك مجلس إدارة رسمياً ووحدة تدقيق داخلي رسمية خاصة بها. وعلى الرغم من عدم وجود نص صريح في كل من قواعد قانون ساربنز أوكسلي SOX وهيئة الأوراق المالية والبورصة الأمريكية يُلزم بذلك، فإن هذه المؤسسات ستستفيد أيضاً من لجنة التدقيق المكونة من مجموعة من المديرين المستقلين.

تتحمل لجنة التدقيق المسؤولية الكاملة عن مهام التدقيق الداخلي والخارجي للمؤسسة. فالمسؤولية الرئيسية للمدققين الخارجيين تجاه مجلس إدارة المؤسسة هي التصديق على دقة ونزاهة البيانات المالية. وعلى الرغم من استقلالية المدققين الخارجيين، فإن لجنة التدقيق تقوم بمراجعة الميزانيات الخاصة بالتدقيق الخارجي والتصديق عليها، كما تقوم باستلام التقارير الصادرة عنهم، وسيكون لها اتصالات مستمرة مع الشريك المسؤول عن عملية التدقيق. وعلى الرغم من أن مكاتب التدقيق الخارجي قد تقوم بخدمة إحدى المؤسسات على مدى عدة سنوات، فإنه يحق للجنة التدقيق القيام بتغيير المدققين الخارجيين في حال وجود خلافات حول الخدمات والميزانيات، أو غيرها من المسائل.

إن لجنة التدقيق هي المسؤولة عن التدقيق الداخلي وعن مدققي تقنية المعلومات لديها، والذين يلعبون دوراً كبيراً في عملية تقييم الضوابط الداخلية الموضوعة للتحقق من مدى موثوقية كل من التقارير المالية وعمليات تقنية المعلومات، وفاعلية وكفاءة العمليات التشغيلية، ومدى التزام المؤسسة بالقوانين واللوائح المعمول بها. ويقوم المدققون الداخليون وأخصائيو تدقيق تقنية المعلومات على وجه الخصوص بتقييم العديد من المخاطر المتعلقة بأمن وسلامة تقنية المعلومات وقضايا حوكمة تقنية المعلومات التي تواجه المؤسسة.

إن الإدارات الخاصة بالتدقيق الداخلي تكون محكومة من خلال الميثاق الذي تمت الموافقة عليه من قبل لجنة التدقيق، والذي يحدد أنشطتها وعلاقتها مع لجنة التدقيق في المؤسسة. وتتطلب تلك المواثيق عادة بأن تقوم لجنة التدقيق بالتالي:

- مراجعة الموارد والخطط والأنشطة، والتوظيف، والهيكل التنظيمي الخاص بوحدة التدقيق الداخلي في المؤسسة. وبالنسبة للأنشطة المتعلقة بحوكمة تقنية المعلومات، فقد تم إيجاز هذه المجالات في الفصل التاسع عشر من هذا الكتاب.

- مراجعة عمليات تعيين مدير التدقيق CAE وأدائه وتغييره، وهو الموظف المسؤول عن التدقيق الداخلي.
- مراجعة جميع عمليات التدقيق والتقارير المعدة من قبل وحدة التدقيق الداخلي بجانب مراجعة رد الإدارة.
- مراجعة مدى كفاية التقارير المالية ونظم الرقابة الداخلية مع كل من الإدارة ومدير التدقيق والمحاسبين المستقلين. ويتضمن ذلك نطاق ونتائج برنامج التدقيق الداخلي، والتعاون المتاح أو القيود (إن وجدت) التي كانت تفرضها الإدارة على سير عمليات برنامج التدقيق الداخلي.

ومع مرور الوقت شكلت هذه المتطلبات جزءاً من العلاقة التي تربط ما بين وحدة التدقيق الداخلي ولجنة التدقيق لديها. حيث يجب أن يعمل مدير التدقيق عن قرب مع لجان التدقيق للتأكد من مدى ملاءمة وكفاية الروابط الفعالة للاتصالات. والنقطة الثالثة المذكورة حول تقارير التدقيق تعد خير مثال على ذلك. فقبيل ظهور قواعد قانون ساربنز أوكسلي SOX، كانت بعض إدارات التدقيق الداخلي تقوم بتسليم لجان التدقيق التابعة لها فقط بعض الملخصات المتعلقة بنتائج تقارير التدقيق الداخلي، أو أنها كانت تقوم بتسليم نتائج تقارير التدقيق الداخلي التي يراها مدير التدقيق CAE بأنها "هامة". أما الآن فبموجب قواعد قانون ساربنز أوكسلي SOX، يجب على التدقيق الداخلي أن يزود لجنة التدقيق بجميع تقارير التدقيق وردود الإدارة الداعمة لها، ويتضمن ذلك أحياناً بعض التقارير التي تعتبر فنية إلى حد ما خاصة بتدقيق تقنية المعلومات التي تحتفظ بها إدارة التدقيق الداخلي، والتي جاءت من مراجعي لجنة التدقيق.

لا تشارك لجنة التدقيق عادة بالأعمال الإدارية اليومية الخاصة بإدارة التدقيق الداخلي ومديرها التنفيذي CAE، ولكنها يجب أن تضمن الجودة المستمرة لإدارة التدقيق الداخلي. فعلى سبيل المثال، يجب أن تقوم لجنة التدقيق بمراجعة خطط التدقيق السنوية بعناية، وأن تقوم بتوجيه الأسئلة المناسبة بشأن النتائج والتوصيات التي جاءت في تقارير التدقيق الداخلي. هذا بالإضافة إلى قدرة لجنة التدقيق على تعيين أو فصل مدير التدقيق CAE.

غير أنه يلزم وجود مستوى من التعاون المستمر في هذا الشأن. إذ لا تتواجد لجنة التدقيق في الموقع بشكل يومي لتوفير الإشراف التفصيلي على عملية التدقيق الداخلي ويجب أن تعتمد على الإدارة العليا للمؤسسة من أجل الحصول على بعض الدعم التفصيلي.

لا يستطيع مدير التدقيق أو المدققون الداخليون تجاهل الطلبات الإدارية الملائمة بدعوى أنهم مسؤولون فقط عن توجيه تقاريرهم إلى لجنة التدقيق، وبأنهم غير معنيين بالمسار الإداري للمؤسسة. وبالمثل، فإنه يجب على إدارة المؤسسة أن تكون واثقة من أن وحدة التدقيق الداخلي هي جزء من المؤسسة وليست وحدة خارجية أو غريبة عنها بسبب علاقتها مع لجنة التدقيق.

مسؤوليات لجنة التدقيق تجاه حوكمة تقنية المعلومات:

يجب أن تقوم لجنة التدقيق بتطوير فهم شامل لمجمل احتياجات التدقيق في المؤسسة. ويشتمل هذا التقييم العالي المستوى للاحتياجات على مختلف القضايا الخاصة بالرقابة والتقارير المالية، الأمر الذي يسمح للجنة التدقيق بالقيام بتحديد الاحتياجات الخاصة بالتدقيق أو تقييم المخاطر، والتي ستنفذ إما بواسطة وحدة التدقيق الداخلي أو بواسطة مقدمي خدمات تدقيق آخرين. إن لجنة التدقيق باعتبارها جزءاً من هذا الدور وباعتبارها المنسق النهائي لمجمل الجهود المبذولة في عملية التدقيق، هي المسؤولة عن مراجعة واعتماد الخطط والميزانيات العالية المستوى الخاصة بالتدقيق الداخلي. وعلى الرغم من أنه قد يكون لدى إدارة المؤسسة أفكارها الخاصة بأعمال التدقيق والكيفية التي يجب أن تُنفذ من خلالها تلك الأعمال، وعلى الرغم من المرئيات الخاصة للمدير التنفيذي للتدقيق CAE بخصوص الاحتياجات التي يجب أن تنفذ، فإن لجنة التدقيق هي المسؤولة عن التصديق على الخطط والموازنات الخاصة بوحدة التدقيق الداخلي. ولا بد من أخذ جميع المرئيات أو الآراء المختلفة للأطراف الرئيسية بالاعتبار والعمل على تحقيق التوافق والانسجام فيما بينها بشكل مناسب، إلا أن لجنة التدقيق هي صاحبة الكلمة الأخيرة والفاصلة في هذه المسائل.

وكما وضحنا في الفصول السابقة، كانت الإدارة العليا ولجنة التدقيق التابعة لمجلس الإدارة تهتم عادة بقواعد المحاسبة المالية، وقواعد قانون ساربنز أوكسلي SOX، والقواعد

الشاملة لحوكمة الشركات، أكثر من اهتمامها بالمسائل الخاصة بحوكمة تقنية المعلومات. ويتم تحديد هذه الأنشطة من خلال الخطة السنوية للتدقيق الداخلي التي يتم إعدادها بواسطة وحدة التدقيق الداخلي والموافقة عليها واعتمادها من قبل لجنة التدقيق.

تعتبر المراجعات التي تقوم بها لجنة التدقيق لجميع خطط التدقيق الداخلي هامة وضرورية لتحديد السياسات والخطط المستقبلية على نحو أكثر فاعلية. لذا يجب أن تتولى لجنة التدقيق هذا الدور التنسيق الرفيع المستوى، حتى تتمكن جميع الأطراف المعنية (كإدارة المؤسسة، والمدققين الداخليين، والتدقيق الخارجي على حد سواء) من تحقيق مستوى فهم ومعرفة أفضل لطبيعة وآلية مجمل خطة التدقيق الداخلي، وما يمكن توقعه من مقدمي خدمات التدقيق. وعلى الرغم من وجود قيود عملية على الكيفية أو الطريقة التي يمكن من خلالها إشراك لجنة التدقيق في العملية التفصيلية للتخطيط على نحو فعال، فإن بعض هذه المشاركات أعطت قيمة عالية لعملية التخطيط. وقد جرت العادة بأن يكون رئيس لجنة التدقيق هو الشخص الأكثر فاعلية في هذه العملية الخاصة بمراجعة الخطة، ولكن حتى هذا الشخص يتقيد في عمله هذا بمدد زمنية. لذا يجب أن تقوم وحدة التدقيق الداخلي بإعداد وتحضير مجموعة كاملة من الوثائق التفصيلية المتعلقة بالخطط السنوية، وأن تقوم بتقديمها للجنة التدقيق التي ستقدم بدورها خططاً تفصيلية للسنة القادمة وخططاً مستقبلية طويلة المدى. كما يجب أن تقوم وحدة التدقيق الداخلي أيضاً بإعداد تقارير موجزة عن أنشطة التدقيق وعمليات إعادة التقييم السابقة للمناطق التي قامت بتدقيقها لإعطاء لجنة التدقيق صورة واضحة عن المناطق الهامة التي تمت تغطيتها في المراجعات السابقة. وعلى الرغم من أنه يجب على وحدة التدقيق الداخلي أن تقوم بإعداد تقرير خاص بأنشطتها وإرساله إلى لجنة التدقيق بشكل منتظم، فإن هذا التقرير الموجز للنشاط السابق يعطي لمحة عامة عن المجالات التي تركز عليها عملية التدقيق، ويسلط الضوء أيضاً على أي ثغرات يحتمل ظهورها وقت التدقيق.

ومن منظور حوكمة تقنية المعلومات، قد تتسبب خطط التدقيق الداخلي أحياناً في إثارة مشاكل لأعضاء لجنة التدقيق في المؤسسة. فغالباً ما يجهل هؤلاء الأشخاص أو المديرون

الرفيعو المستوى بعض المسائل المتعلقة بحوكمة تقنية المعلومات التي تم الحديث عنها في فصول هذا الكتاب كإدارة معيار أمن البيانات الخاص بصناعة بطاقات الدفع PCI DSS، والذي تحدثنا عنه في الفصل الحادي عشر من هذا الكتاب. لذا يجب على مدير التدقيق، وبدعم من الفريق الخاص بتدقيق تقنية المعلومات، أن يقوموا باتخاذ المزيد من الخطوات لتثقيف لجنة التدقيق عن سبب تأكدها من أهمية القضايا الأكثر فنية التي تتعلق بتقنية المعلومات من منظور الضوابط الداخلية ومخاطر حوكمة تقنية المعلومات.

اجتماعات لجنة التدقيق وقضايا حوكمة تقنية المعلومات:

قد تكون القضايا والمخاوف المتعلقة بحوكمة تقنية المعلومات غير مألوفة بالنسبة لبعض المديرين العاملين في لجان التدقيق، وذلك من خلال بعض القضايا التي تبدو في بعض الأحيان غريبة بالنسبة إليهم. ويعتاد المديرون التنفيذيون العاملون في لجنة التدقيق غالباً على التعامل مع عدد محدود من القضايا المتعلقة بحوكمة تقنية المعلومات حتى أصبحت مألوفة بالنسبة لهم، مثل أهمية الخطط الفعالة لاستمرارية تقنية المعلومات، والمسؤوليات القانونية المحتملة الناجمة عن قضايا حوسبة الشبكة الاجتماعية، أو المخاطر المتعلقة بفيروسات البرمجيات. وقد تحدثت العديد من منشورات الأعمال الموجهة للمديرين التنفيذيين في لجنة التدقيق عن أنواع المخاطر وقضايا حوكمة تقنية المعلومات المتعلقة بها. ومع ذلك، فإنه يجب على كل من الإدارة العليا ومدير التدقيق ووحدة تدقيق تقنية المعلومات، أن يقوموا بمحاولة إيصال مخاوفهم المتعلقة بالقضايا الأكثر تقنية وقضايا الحوكمة المرتبطة بها إلى أعضاء لجنة التدقيق.

تعد خطط مراجعة تدقيقات حوكمة تقنية المعلومات والمخاوف المتعلقة بالمخاطر جزءاً من الخطط الإجمالية لعمليات التدقيق الداخلي، لذا يجب أن يكون هناك اتصال مفتوح بين مدققي تقنية المعلومات ومديريهم التنفيذيين فيما يخص تلك القضايا المحددة في حوكمة تقنية المعلومات. ومع ذلك فإن إرسال الخطابات إلى لجنة التدقيق تعتبر في بعض الأحيان مشكلة كبيرة. وكما تحدثنا سابقاً، فإن أعضاء لجنة التدقيق مشغولون تماماً أكثر بالقضايا التي تتعلق بالتقارير المالية والالتزام بقانون ساربنز أوكسلي SOX وغيرها من قضايا المخاطر الأخرى، ولا يركز العديد منهم على قضايا التدقيق الداخلي المرتبطة بحوكمة

تقنية المعلومات بشكل منتظم. وبالاستعانة بمدير التدقيق، تحتاج عملية تدقيق تقنية المعلومات إلى أن تصل إلى أعضاء لجنة التدقيق لتطلعهم على أهمية القضايا المتعلقة بالضوابط الداخلية لحوكمة تقنية المعلومات ومدى تطورها.

وقد يكون من المجدي أو من الأهمية بمكان بالنسبة للعديد من المؤسسات أن تقوم بجدولة اجتماعات توجيهية ربع سنوية (كل ثلاثة أشهر) مع لجنة التدقيق لإطلاعهم على المخاطر والمستجدات المتعلقة بحوكمة تقنية المعلومات. ويمكن استغلال هذه الاجتماعات لتثقيف أعضاء لجنة التدقيق عن قضايا بيئة حوكمة تقنية المعلومات في المؤسسة وغيرها من القضايا المتعلقة بالمخاطر. ويمكن أحياناً تنفيذ هذا النوع من الاجتماعات بالاشتراك مع المدير التنفيذي للمعلومات في المؤسسة، لكن في كثير من الأحيان نرى أنه من الأفضل أن يتم قيادة الجلسة في المقام الأول من قبل مدير التدقيق ووحدة تدقيق تقنية المعلومات في المؤسسة.

إن المسؤولية العظمى التي تقع على عاتق لجنة التدقيق هي القيام بمراجعة النتائج الهامة لعمليات التدقيق التي تصل إليها عن طريق المدققين الداخليين والخارجيين والإدارة وغيرهم، وأن تقوم باتخاذ التدابير المناسبة حيالها. ومع أن لجنة التدقيق تتحمل المسؤولية عن كل هذه المجالات، إلا أن تركيزنا هنا ينصب على الحاجة إلى لجنة تدقيق تقوم بعمليات التدقيق الداخلي وتدقيق تقنية المعلومات على وجه الخصوص، وذلك لمراجعة وفهم جميع النتائج والقضايا المتعلقة بحوكمة تقنية المعلومات التي تصل لأعضاء اللجنة واتخاذ التدابير المناسبة المنتظمة والفورية.

إن الرد على النتائج الهامة لعملية التدقيق التي تم إيصالها إلى لجنة التدقيق يتطلب مزيجاً من الفهم، والكفاءة، والتعاون من قبل جميع الأطراف الرئيسية المعنية، وهي التدقيق الداخلي، والإدارة، والمدققين الخارجيين، ولجنة التدقيق نفسها. ويصبح بعد ذلك مستوى الرفاهية في المؤسسة هو المعيار الحقيقي الذي نحكم من خلاله على جميع خدمات التدقيق الداخلي، على عكس العديد من المرنّيات المحلية التي ترى احتمالية تعارض مصالح كل من الإدارة ولجنة التدقيق. كما يجب على إدارة تقنية المعلومات، في حدود مسؤوليتها، أن تعمل بجد بتطبيق التدابير التحسينية المستمرة للحوكمة لتقييم ما إذا كانت البنود المناسبة للإجراء التصحيحي في مكانها الصحيح.

لقد تحدث هذا الفصل والفصول السابقة من هذا الكتاب عن مجموعة واسعة من القضايا الخاصة بحوكمة تقنية المعلومات التي تؤثر في مؤسسات الأعمال. وعلى الرغم من أن لجنة التدقيق هي المسؤولة في نهاية المطاف عن تقييم التقدم والأنشطة المتعلقة بهذه الأمور، فإنه يجب على الإدارة العليا المسؤولة عن حوكمة تقنية المعلومات في المؤسسة أن تحدد ما إذا كان قد تم تثبيت ووضع العمليات المناسبة، وما إذا كانت تلك العمليات تعمل بالشكل الصحيح. إن النظام الجيد لضوابط وعمليات حوكمة تقنية المعلومات سوف يسهم في نجاح المؤسسة بشكل عام.

نبذة عن المؤلف:

روبرت ر. مولر، حاصل على شهادات CPA و CISA و CISSP و PMP، وهو متخصص في التدقيق الداخلي ونظم الرقابة الداخلية وإدارة المشاريع، ولديه فهم جيد لحوكمة الشركات ونظم المعلومات وإدارة المخاطر. تمتد خبرته لأكثر من ٤٠ عاماً في إدارة وحدات التدقيق الداخلي وإدارة مجموعة واسعة من مشاريع تقنية المعلومات وغيرها من المشاريع من خلال نظم الرقابة الداخلية والحوكمة. عمل مديراً وطنياً لتدقيق تقنية المعلومات لشركة جرانت ثورنتون (Grant Thornton)، كما كان مدير التدقيق الداخلي لشركة سيرز روبوك (Sears Roebuck)، حيث كان يرفع تقاريره للجنة التدقيق وترأس فريقاً لإعادة هيكلة عمليات الرقابة الداخلية للمؤسسة وكان أول من أنشأ إدارة أخلاقيات شركتهم. يعد الكاتب مؤلفاً ومتحدثاً مشهوراً، فهو يقدم لقارئيه رؤى ثاقبة لعدد من قضايا الأعمال ومخاوفها التي تؤثر في عمليات الحوكمة والمخاطر والامتثال في المؤسسة.

المترجم في سطور

١- محمد أحمد عبداللطيف أحمد

المؤهل العلمي:

• ماجستير علوم الحاسب، جامعة المنيا، مصر عام ٢٠٠٩ م.

العمل الحالي:

• عضو هيئة تدريس، قطاع تقنية المعلومات، معهد الإدارة العامة، الرياض.

الأنشطة العلمية والعملية:

- باحث بقسم علوم الحاسب، كلية العلوم، جامعة المنيا، ٢٠٠٤-٢٠٠٦.
- عضو فريق مشروع إنشاء مركز دعم نظم المعلومات الإدارية، جامعة المنيا، ٢٠٠٦-٢٠١٠.
- تصميم وإعداد ومراجعة عدة حقائب تدريبية، معهد الإدارة العامة - قطاع تقنية المعلومات.
- حاصل على العديد من الشهادات الاحترافية الدولية في مجال تقنية المعلومات وإدارتها وحوكمتها.
- مدرب معتمد من شركة ميكروسوفت.

إضافة إلى هذا الكتاب لدى المترجم عدد من الأبحاث العلمية:

- 1- Ahmed. A. A. Radwan, Fatma A. Omara, A. A .Ali, M. A. Abdelatif, "Enhanced Distributed QoS Routing Algorithms in Wireless Networks", International Journal of Intelligent Computing & Information Sciences, Vol.8, No.2, (July2008) pp223-235
- 2- Ahmed. A. A. Radwan, Fatma A. Omara, A. A .Ali, M. A. Abdelatif, "Distributed QoS Routing Using Developed Flooding in Wireless Ad

Hoc Networks”, The proceeding of the fourth International Conference on Intelligent Computing and Information Systems (ICICIS) 19-22 March 2009, pp. 490-501, Cairo-Egypt

- 3- Mohamed A. El-Sayed, M. Hassaballah, Mohammed A. Abdel-Latif, "Identity Verification of Individuals Based on Retinal Features Using Gabor Filters and SVM", Journal of Signal and Information Processing, Vol.7 No.1, February 2016, pp.49-59
- 4- Mohamed A. El-Sayed, Mohammed A. Abdel-Latif, "Optimization Methods for Identity Verification System Using Biometric Features", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 18 (2017) pp. 7143-7153

٢- عبدالله حسن كامل صالح

المؤهل العلمي:

- ماجستير في علوم الحاسب الآلي والبرمجة من الجامعة الأردنية، عمان، الأردن، عام ٢٠٠١ م.

العمل الحالي:

- مدرب في قطاع برامج الحاسب في معهد الإدارة العامة - المركز الرئيسي في الرياض.
- مسئول عن تقديم الدعم الفني والتقني للأنظمة المالية والموارد البشرية الخاصة بتطبيق أنظمة التخطيط للموارد المؤسسية ERP في معهد الإدارة العامة في المركز الرئيسي في الرياض.

الأنشطة العلمية والعملية:

- عضو هيئة تدريس (محاضر) في كلية تقنية المعلومات - جامعة فيلادلفيا في الأردن من عام ٢٠٠١ إلى عام ٢٠٠٨.
- عضو هيئة تدريب (مدرب) في معهد الإدارة العامة - المركز الرئيسي - الرياض من عام ٢٠٠٨ إلى الآن.
- تصميم ومراجعة عدة حقائب تدريبية في معهد الإدارة العامة - قطاع تقنية المعلومات.
- عضو في لجنة إعداد الخطة الإستراتيجية لتقنية المعلومات في معهد الإدارة العامة المنفذة منذ العام ١٤٣٥/١٤٣٦ هـ إلى عام ١٤٤٠ هـ.
- عضو في فريق إعداد معايير نشاط الاستشارات في معهد الإدارة العامة بالتنسيق مع الهيئة الوطنية للتقويم والاعتماد الأكاديمي في وزارة التعليم.

مراجع الترجمة في سطور

د. محمد بن عبدالله الشنيفي

المؤهل العلمي:

دكتوراه الفلسفة في علوم الحاسب الآلي، مايو ١٩٩٨،
معهد إلينوي للتكنولوجيا، شيكاغو، إلينوي.

العمل الحالي:

- أستاذ مشارك في قسم هندسة علوم الحاسب الآلي، كلية علوم الحاسب وتقنية المعلومات،
جامعة الباحة. ديسمبر ٢٠١٦ إلى الوقت الحاضر.

أبرز لأنشطة العلمية:

- Hisham Al-Mubaid, Sasikanth Potu¹, and M. Shenify. Determining Multifunctional Genes and Diseases in Human Using Gene Ontology. 9th International Conference on Bioinformatics and Computational Biology (BICOB 2017) Honolulu, Hawaii, USA. March 20 – 22, 2017.
- Duong B. Nguyen, Mohamed Shenify, and Hisham Al-Mubaid¹. Biomedical Text Classification with Improved Feature Weighting Method. 8th International Conference on Bioinformatics and Computational Biology (BICoB) Las Vegas, Nevada, USA. April 4-6, 2016.
- H. Al-Mubaid. Mohamed Shenify and Sultan Aljahdali. Assessing Gene-Disease Relationship with Multifunctional Genes Using GO. Accepted paper. IEEE AICCSA 2016.
- H. Al-Mubaid, and Mohame Shenify . Improved Bayesian based method for classifying disease documents. WSCAR-2016
- Bassam Naji Al-Tamimi, Mohammed Shenify, Rahmat Budiarto, A New Algorithm For Protecting Mobile Home Network From IPv6 Routing Header Vulnerability In Mixed IP Networks, Journal of ICT, UUM Press, Vol. 14, 2015 (to appear)

- Mohamed Shenify and Foukrul Alom Mazarbhuiya. The Expected Value of Fuzzy Number. International Journal of Intelligence Science, 2015, Vol. 5, Pp. 1-5.
- M. Shenify. Extracting Cyclic Frequent Set from Fuzzy Temporal Data. 30th International Conference on Computers and Their Applications CATA-2015, March 9-11, 2015. Honolulu, Hawaii, USA.
- M. Shenify and F. A. Mazarbhuiya. Discovering Monthly Fuzzy Patterns. International Journal of Intelligence Science, 2015, Vol.5, Pp. 37-43.
- Ali Alshehri, Naif Hamed Almutairy, El-Sayed Osman, Mohamed Shenify and, Rahmat Budiarto, 2015, Improvement of Teaching Listening English as Secondary Language Using Student Response Systems, A Case Study at King Fahd Secondary School in Albaha: Towards Informed Teacher Decisions, Proceedings of the Albaha University and Uppsala University Symposium on Quality in Computing Education (ABU3QCE 2015), Albaha, KSA, 24-25 February 2015, Pp.47-51 (<http://www.abu3qce.al-aqiq.com/proceedings.pdf>)
- Bassam Naji Al-Tamimi, Mohammed Shenify, Rahmat Budiarto, Protecting, Home Agent Client from IPv6 Routing Header Vulnerability in Mixed IP Networks , Journal of ICT, UUM Press, Vol. 14, 2015, Pp.77-93.
- Mohammed Shenify, Rahmat Budiarto, Sultan Aljahdali, Hisham M. Alsaghie, 2015, Incorporating R&D Activities into Computer Engineering Teaching & Learning Program in Albaha University, Proceedings of The 3rd International Conference on Learning and Teaching in Computing and Engineering (LaTiCE, IEEE Technically Sponsored) 2015, Taipei, 9-12 April 2015
- F.A. Mazarbhuiya, M.Shenify. An Efficient Alogrithm for Mining Locally Frequent Itemsets.2014 ASE BIGDAT/SOCIAL COM/CYBERSECURITY, Conference, Stanford University, May, 27-31, 2014. ISBN: 987-1-62561-000-3.
- Mohamed Shenify, Language Variation: Corpus Evaluation using Language Modeling, International Computing Conference in Arabic :ICCA 2013, 9-10-11, December, 2013.Tunisia.

- Mohamed Shenify Geographical Classification for Arabic text. International Computing Conference in Arabic :ICCA 2013, 9-10-11, December,2013 .Tunisia
- Mohamed Shenify, Trusted Node-Based Algorithm to Secure Home Agent NATed IPv4 Network from IPv6 Routing Header Attacks, TELKOMNIKA journal, Vol.12, No.4, December 2014, Pp. 969-976 (http://journal.uad.ac.id/index.php/TELKOMNIKA/article/view/540/pdf_51)
- Mohamed Shenify, Retrieving Information Using Concept For Multi-Format Data In Cloud Environment, Submitting to JTAIT
- Zahra Eskandari, Seyed Amin Hosseini Seno, Muhamed Shenify, Rahmat Budiarto, 2014, Optimal Cluster Head selection in Wireless Sensor Networks using Integer Linear Programming Techniques, International Journal of Informatics and Communication Technology (IJ-ICT), IAES ISSN: 2252-8776, Vol 3(3), DOI: 10.11591/ij-ict.v3i3.6614
(<http://iaesjournal.com/online/index.php/IJICT/article/view/6614>)
- Alireza Tajalli, Seyed-Amin Hosseini-Seno and, Mohamed Shenify, Rahmat Budiarto, 2014, An Incentive Mechanism for Cooperative Data Replication in MANETs A Game Theoretical Approach, Proceedings of International Conference Electrical Engineering, Computer Science and Informatics (EECSI 2014), Yogyakarta, Indonesia, 20-21 August 2014, Pp.111115 (<http://iaesonline.com/eecsi/2014/>)
- Fatemeh Hakimifar ,Seyed-Amin Hosseini-Seno, Mohamed Shenify and Rahmat Budiarto, 2014, An Efficient Cluster-based Routing Protocol for Mobile Ad Hoc Networks, Proceedings of International Conference Electrical Engineering, Computer Science and Informatics (EECSI 2014), Yogyakarta, Indonesia, 20-21 August 2014, Pp.476-481 (<http://iaesonline.com/eecsi/2014/>)
- F. A. Mazarbhuiya, M. Shenify, A. Khan, A. Farooq. Finding Cyclic Frequent Itemsets. IJCSI International Journal of Computer Science, 2012, Vol. 9, issue 6 (1), 229-236.
- Soraya Zaidi, Ahmed Abdelali, Mohamed-Tayeb Laskri, Mohamed A. Al Shenify. Extracting Simple and Compound Terms from Arabic Texts: An Application on The Quranic Text. Communication of the Arab Computer Society, 2011, vol. 4(1).

-
- Mu'away Naser and Mohammd Al-Shnify. Blood Vessels Segmentation From Liver CT Scan Image Using Level Set Curve Evolution. G. J. P&A Sc and Tech., 2011, vol. 1(2), Pp. 38-55.
 - Mohammed Shenify, Rahmat Budiarto, Sultan Aljahdali, Hisham M. Alsaghie, 2015, Incorporating R&D Activities into Computer Engineering Teaching & Learning Program in Albaha University, Proceedings of The 3rd International Conference on Learning and Teaching in Computing and Engineering (LaTiCE, IEEE Technically Sponsored) 2015, Taipei, 9-12 April 2015.

حقوق الطبع والنشر محفوظة لمعهد الإدارة العامة ولا يجوز
اقتباس جزء من هذا الكتاب أو إعادة طبعه بأية صورة دون موافقة
كتابية من المعهد إلا في حالات الاقتباس القصير بغرض النقد
والتحليل، مع وجوب ذكر المصدر.

تم التصميم والإخراج الفني والطباعة في
الإدارة العامة للطباعة والنشر بمعهد الإدارة العامة - ١٤٤٠هـ

هذا الكتاب:

يزداد الاهتمام بالحوكمة من قبل جميع الشركات على اختلاف أحجامها وأنواعها. سواء كانت مؤسسات قطاع عام لا تهدف للربح أم كيانات خاصة. وذلك في ظل الظروف الاقتصادية الدائمة التغير التي يشهدها عالم اليوم. وتتكون مفاهيم حوكمة المؤسسات من سلسلة من مجالات واسعة تغطي جميع أنشطة المؤسسة، والتي يتطلب تطبيقها عدداً من الإرشادات والبرامج لضمان نزاهة الإجراءات الإدارية وحماية المؤسسة من الممارسات المخالفة والاحتيالية. ومن الطبيعي أن تحتاج الحوكمة المؤسسية الفعالة إلى مهارات إدارية قوية لاتخاذ قرارات مهمة. كما تحتاج احتياجاً كبيراً إلى نظم وعمليات تقنية المعلومات على وجه الخصوص. ويمثل هذا المجال المهم حوكمة تقنية المعلومات. وهو الموضوع الشامل لهذا الدليل التنفيذي.

يتناول هذا الكتاب مفهوم حوكمة تقنية المعلومات. الذي يُعد جزءاً من مفاهيم حوكمة المؤسسات. فهو يهدف إلى تقديم معلومات أساسية عن القضايا المتعلقة بحوكمة تقنية المعلومات. وقد تم تقسيم الكتاب إلى ستة أجزاء رئيسية يتناول كل جزء منها عدداً من القضايا التي تخص حوكمة تقنية المعلومات.

إن الهدف العام من هذا الكتاب يتمثل في مساعدة كبار مديري المؤسسات على فهم أهمية قضايا حوكمة تقنية المعلومات فهماً أفضل وتطبيقها في مؤسساتهم. من خلال تزويدهم بالمعايير وأطر العمل العالمية اللازمة للوصول إلى نظم وعمليات أقوى لكل من تقنية المعلومات والمؤسسة بأكملها.



9 9 6 0 1 4 2 8 7 6